NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEFENSIVE SWARM: AN AGENT-BASED MODELING ANALYSIS

by

Nathan E. Padgett

December 2017

Thesis Advisor: Camber Warren
Co-Advisor: Duane Davis

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE DEFENSIVE SWARM: AN AGENT-BASED MODELING ANALYSIS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Nathan E. Padgett	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Security at remote military bases is a difficult, yet critical, mission. Remote locations are generally closer to enemy combatants and farther from supporting forces; the individuals charged with defending the bases do so with less equipment. These locations are also usually reliant on air-resupply missions to maintain mission readiness and effectiveness. This thesis analyzes how swarms of small autonomous unmanned aerial vehicles (UAVs) could assist in defensive operations.

To accomplish this, I created an agent-based computer simulation model, which creates a tactical problem (enemies attempting to attack or infiltrate a notional base) that a swarm of UAVs attempts to defend against. Results indicate that a swarm can effectively deter 95% of attackers if each UAV is responsible for covering no more than 0.18 square miles and at least 40% of the UAVs are armed. I conclude that UAVs are an excellent addition to base defense and are particularly helpful at remote outposts with less organic capability (limited field of view, defensive assets, etc.). While this research deals specifically with countering a threat to a central base, the algorithms for swarm dynamics could be applied to future problems in mobile convoy or aircraft defense, and even peacetime applications like search and rescue.

14. SUBJECT TERMS agent, modeling, agent-based model, ABM, drone, unmanned, swarm, swarming, UAV, UAS, base defense, generalized-linear model, GLM, receiver operating characteristic, ROC	**15. NUMBER OF PAGES** 121
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DEFENSIVE SWARM: AN AGENT-BASED MODELING ANALYSIS

Nathan E. Padgett
Major, United States Air Force
B.S., Georgia Institute of Technology, 2005
M.A., American Military University, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Dr. Camber Warren
Thesis Advisor

Dr. Duane Davis
Co-Advisor

Dr. John Arquilla
Chair, Department of Defense Analysis
Graduate School of Operational and Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Security at remote military bases is a difficult, yet critical, mission. Remote locations are generally closer to enemy combatants and farther from supporting forces; the individuals charged with defending the bases do so with less equipment. These locations are also usually reliant on air-resupply missions to maintain mission readiness and effectiveness. This thesis analyzes how swarms of small autonomous unmanned aerial vehicles (UAVs) could assist in defensive operations.

To accomplish this, I created an agent-based computer simulation model, which creates a tactical problem (enemies attempting to attack or infiltrate a notional base) that a swarm of UAVs attempts to defend against. Results indicate that a swarm can effectively deter 95% of attackers if each UAV is responsible for covering no more than 0.18 square miles and at least 40% of the UAVs are armed. I conclude that UAVs are an excellent addition to base defense and are particularly helpful at remote outposts with less organic capability (limited field of view, defensive assets, etc.). While this research deals specifically with countering a threat to a central base, the algorithms for swarm dynamics could be applied to future problems in mobile convoy or aircraft defense, and even peacetime applications like search and rescue.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABM	agent-based modeling
AI	artificial intelligence
AIC	Akaike information criterion
BLOS	beyond line of sight
C2	command and control
DA	direct action
ISR	information, surveillance, and reconnaissance
JSA	joint security area
JSO	joint security operations
LOS	line of sight
NMS	National Military Strategy
NSS	National Security Strategy
OOP	object-oriented programming
RTB	return to base
ROC	receiver operating characteristic
SOF	Special Operations Forces
UAS	unmanned aircraft (aerial) systems
UAV	unmanned aerial vehicle
UCAV	unmanned combat aerial vehicle
USAF	United States Air Force
VEO	violent-extremist organizations

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To begin, I must say that I am incredibly thankful for the opportunity to have attended the Naval Postgraduate School and certainly to have been in the Defense Analysis Department. All of my instructors and mentors assisted in my academic development and ability to apply distinct lenses to various types of problems. The entirety of my time at NPS was wonderful for me and for my family.

For this specific project, I would like extend my sincerest appreciation to Dr. Timothy (Camber) Warren for his guidance during both the formulation of this project and throughout its development. His particular knowledge of agent-based modeling and underlying methods of analysis was instrumental in shaping the research and how I was able to work through various challenges with the material. His instruction on, and assistance with, evaluating statistical models proved vital to formulating conclusions and recommendations. Lastly, Dr. Warren's ability to parse arguments and data was an incredibly welcome addition to the final stages of the thesis process.

Dr. Duane Davis, and his previous work on UAV swarm dynamics and interoperation, provided the foundation of my understanding of swarm architecture and communication. His willingness to provide sample code and instruction on UAV interoperation enabled me to have a launching point to begin my research and code development. My hope is that some of this work will provide Dr. Davis with additional features for his research and assist him in continuing to develop military minds at the service academies and the Naval Postgraduate School (NPS). Only through advanced research and developed skillsets will the U.S. military continue to be able to succeed in future conflicts.

Unattached, but to some degree indispensable, to this project was Dr. Thomas Otani. Dr. Otani instructed a course in Python programming at NPS, which was a welcome return to the computer science discipline for me. His attention to detail, continuous call for improved algorithms, and education helped me to learn enough of Python to be able to work on this project.

Finally, I present my family with unending gratitude for their support during this project. My wife assisted me greatly during this effort by providing support, an "interested" ear, and a calming presence during many moments of frustration with what our 4-year-old refers to as my "computer robots." My wife's persistent ability to assist me with handling a wide variety of issues across a spectrum of topics is essential to any endeavor I set forth on. I am forever grateful to have had her, and two intelligent little girls, along for this portion of my academic life.

I. INTRODUCTION

A. BACKGROUND

1. Strategic Situation

The current endeavors by the United States against violent-extremist organizations (VEOs), appear to be increasingly reliant on small-force capabilities and U.S. Special Operations Forces (SOF). Rapid advances in commercially-available electronics technology during the last 25 years have resulted in non-state actors (NSA) being able to acquire devices that deliver instant communication, localized intelligence, surveillance, and reconnaissance (ISR) capability, and remote kinetic engagement. To combat this type of enemy, U.S. forces rely on traditional forms of intelligence gathering, human networks and relationships, and national ISR assets. These national assets, however, are not always available to SOF and other elements working in remote locations. As U.S. forces continue to operate in austere environments, it will become increasingly important for small units to be able to generate their own organic ISR and limited fires using small airborne platforms such as unmanned aerial vehicles (UAVs).

The 2015 National Security Strategy (NSS) dictates that the fight against terrorism and VEOs must be accomplished through "a more sustainable approach that prioritizes targeted counterterrorism operations, collective action with responsible partners, and increased efforts to prevent the growth of violent extremism and radicalization that drives increased threats."[1] Here, the executive branch, in response to recognition that the "large-scale ground wars in Iraq and Afghanistan"[2] were not overly effective in combating the spread of VEOs, admits its belief that small forces (like SOF) are likely the best method to target pockets of extremist groups. In addition to direct-action (DA) missions, the NSS also supports further capacity-building operations. It states,

---

[1] Barack Obama, "National Security Strategy 2015" (Washington, DC: Executive Office of the President, February 2015), 9.

[2] Obama, "NSS," 9.

> We will continue to bolster the capacity of the U.N. and regional organizations to help resolve disputes, build resilience to crises and shocks, strengthen governance, end extreme poverty, and increase prosperity, so that fragile states can provide for the basic needs of their citizens and can avoid being vulnerable hosts for extremism and terrorism.[3]

This push for indirect operations is also relevant to SOF operators. SOF forces are, and will continue to be, used in these capacity-building missions and certainly demanded to assist in developing partner forces capable of DA missions against VEOs in austere environments.

The logical marrying of SOF and remotely-operated (unmanned) vehicles was established in the 2015 National Military Strategy (NMS). In the NMS, they are listed in the "decisive advantage"[4] category. It is recognized at the highest echelons of military leadership that these functions are essential to future fights and "[countering Anti-Access/Area Denial], space, cyber, and hybrid threats."[5] The benefits from significant advantages in these areas could result in force-multiplying effects and asymmetric advantages in both conventional and irregular conflicts.

An experienced military planner should quickly recognize that SOF elements will therefore be tasked with objectives falling anywhere along the spectrum of military operations. In order to meet the demands that the NSS and NMS present, SOF elements will be forced to continually innovate ways to create similar effects with potentially fewer personnel or against more sophisticated (resourceful) enemies. An organic drone capability could be an effective measure to support SOF, and other small-force, elements in the field.

SOF operators, like many of their opposing VEO counterparts, often find themselves in remote locations with limited direct-support forces available to assist them.

---

[3] Obama, "NSS," 10.

[4] Joint Chiefs of Staff, "The National Military Strategy of the United States of America 2015," (Washington, DC: Joint Staff Publications, June 2015), 16, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

[5] Joint Chiefs of Staff, "NMS," 16.

Howard explains, "As situations and adversaries become more complex, SOF leaders will need a greater capability for observing their targets. Surveillance, reconnaissance, and communication assets that deliver near-real-time, full-motion video for extended periods of time will be required."[6] Persistent ISR is an enduring request for operators and commanders at every level; this produces increased strain on availability for theater and national assets. Additionally, drones that can perform ISR functions are usually apportioned to operational and strategic-level priority missions, thus leaving some tactical-level operators to work-around the absence of dedicated ISR in ad hoc methods. This tactical capability gap must be addressed and, for it to be ubiquitous, the solution should be relatively inexpensive. With today's technology, this may indeed be possible.

2. Tactical Problem

At remote (austere) airfields, security for both ground personnel and air operations is always a concern. Remote locations are generally closer to enemy combatants, farther from supporting forces, and the individuals charged with defending the bases do so with less equipment. These locations are also usually reliant on air-resupply missions to maintain mission readiness and effectiveness. Because of the remoteness and, often times, increased threat to air operations, combatant commands may restrict operations to try to mitigate potential casualties. These restrictions can severely limit the number and type of aircraft that can operate at a base. Furthermore, organic air operations operate at greater risk due to the limited secure area surrounding the base. Could large clusters (swarms) of small autonomous unmanned-aerial vehicles (UAV) alleviate portions of these problems while also providing increased combat capability (survivability) to both personnel and assets?

UAVs can perform vastly different missions by attaching different components. Swarms could potentially operate as an extended surveillance perimeter augmenting the field-of-view (FOV) from the base, perform limited air strikes, or even enhance missile-

[6] Stephen P. Howard, "Special Operations Forces and unmanned aerial vehicles : sooner or later?," (Maxwell Air Force Base, Alabama: Air University Press, School of Advanced Airpower Studies, 1996), 1, http://aupress.maxwell.af.mil/digital/pdf/paper/t_howard_special_operations_forces.pdf.

warning awareness during aircraft operations. Additionally, traditional barriers to entry (cost, technology, sustainability) for operating small autonomous systems in austere locations are disappearing. Simple, yet capable, small units are continuously developed and improvements in processing power, small optics, and battery life will continue to revolutionize overall ubiquity and functionality.

Remote airfields, however, do not utilize drone swarms for defense because it is an emerging capability that has not become part of any official operational defensive employment strategy. Despite its current absence, emerging evidence exists that swarm behavior is controllable and could be effective in military roles (such as the Marines' Perdix Swarm).[7] Once active, drones could allow for scalable operations, rapid reprogramming on the advent of enemies altering tactics, yet remain (relatively) cheap and replaceable. While many positive outcomes of usage are possible, issues such as over-reliance (complacency), interference with air operations (error or programmed), ethical concerns about autonomous surveillance and strike, and how to eliminate the possibility of fratricide must be also considered.

B. SIGNIFICANCE OF STUDY

It is important to start work on this problem set now because robotic, and likely autonomous, technology will soon dominate the battlefield.[8] One aeronautical expert found that "Unmanned systems are expected to proliferate and the role of the human will increasingly be that of a user and operator more than a controller."[9] This push towards autonomy will lead to incredibly advanced UAVs capable of complex decision making,

---

[7] Department of Defense, "Department of Defense Announces Successful Micro-Drone Demonstration Press Operations," Release No: NR-008-17, January 9, 2017, https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration.

[8] Dan Gonzales and Sarah Harting, *Designing Unmanned Systems with Greater Autonomy: Using a Federated, Partially Open Systems Architecture Approach* (Santa Monica, CA: RAND Corporation, 2014), http://www.rand.org/pubs/research_reports/RR626.html, 2; Penny, Maryse, Tess Hellgren and Matt Bassford, *Future Technology Landscapes: Insights, Analysis and Implications for Defence*, (Santa Monica, CA: RAND Corporation, 2013), 96–101, http://www.rand.org/pubs/research_reports/RR478.html.

[9] Reg Austin, *Unmanned Aircraft Systems: UAVS Design, Development and Deployment* (New York: John Wiley & Sons, Incorporated, 2010), ProQuest Ebook Central, 316.

task management, and even integrated operations with human-operated machines. Already, drones and robotic counterparts are quickly becoming indispensable in fields like ISR and explosive-ordinance disposal, and soon may be common to other disciplines like battlefield-medical evacuation. A failure to address integration with non-human actors, specifically in the air domain, will leave the U.S. in a tactical disadvantage that in the aggregate could also amount to a strategic failure. An enemy able to exploit U.S. defenses because of drone capability (even low-threshold-to-entry solutions such as those adopted by the Islamic State of Syria and Iraq [ISIS][10]), or otherwise able to utilize this space to their own benefit, will gain an asymmetric advantage in a battlespace. Ultimately, we must ask: how can a swarm of drones best support defensive operations at a base?

10 Thomas Gibbons-Neff, "ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say," *The Washington Post*, 14 June 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/?utm_term=.3e1b890ed203.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. DEFINITIONS AND CONCEPTS

While the term 'drone' is convenient and generates a similar image in both academic and military minds, it is not truly an appropriate term for what the robot, or agent, will accomplish in this role. The word 'drone' is also generally associated with its negative connotation concerning dull, mindless speech. Furthermore, when considered militarily, many people consider drones to simply be the physical manifestation of a remote operator hundreds, if not thousands, of miles away from the area of operations. Thus, most encapsulate the drone paradigm with a layer of either mindless monotony or lifeless metal bending to the will of a superior human mind.

In this study, however, the *drone*s I discuss are more accurately termed *UAVs*. Austin defines a UAV as an unmanned aircraft which has "some greater or lesser degree of 'automatic intelligence'. It will be able to communicate with its controller and to return payload data such as electro-optic or thermal TV images, together with its primary state information – position, airspeed, heading and altitude."[11] In this study, I use the term *drone* interchangeably with *UAV*, but am speaking of the higher-functioning variety.

More complex UAVs are often better understood to be part of an Unmanned Aircraft (or Aerial) System (UAS).[12] The UAS is composed of multiple parts (Figure 1) in which the UAV itself is only one piece. The system represents a holistic view and understanding of what enables a UAV to be airborne and accomplish its mission. In a UAS, a particular drone may be a semi- or fully-autonomous agent intentionally performing actions based on its own artificial intelligence (programming) and understanding of a particular environment. It is a being that can act autonomously, under the direct control of an operator, or any mix of the two.

---

[11] Austin, *Unmanned Aircraft Systems*, 3.

[12] Shira Efron, *The Use of Unmanned Aerial Systems for Agriculture in Africa: Can It Fly?* (Santa Monica, CA: RAND Corporation, 2015), 9, http://www.rand.org/pubs/rgs_dissertations/RGSD359.html.

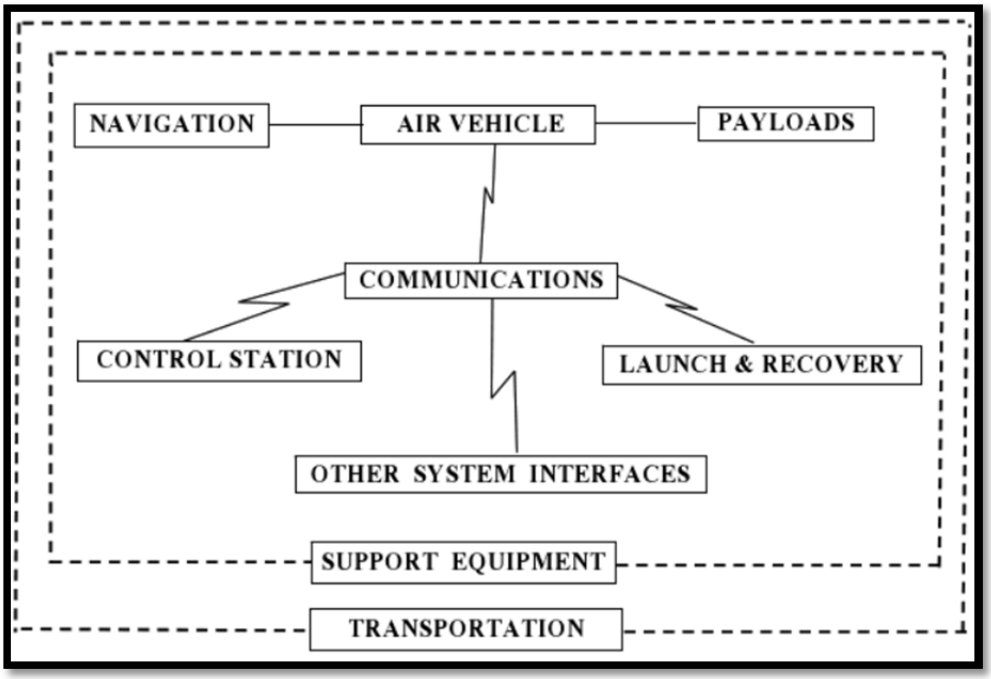


Figure 1. Unmanned Aircraft System[13]

The physical manifestations of the UAV agents addressed in this research fall mainly into Efron's Vertical Takeoff and Landing category (3–180 pounds)[14] and are predominantly on the lower end of that scale. In conventional military nomenclature, they are most like Mini UAVs (under 20 kg), but due to some being armed with air-to-ground ordnance (a grenade), a Mini UCAV (unmanned combat air vehicle) may be more appropriate.[15] Regardless of the UAV's weight, size, or capability, the important piece here is how the agents act and interoperate. While the individual agent is a system on its own, in the sense that it is a complex machine, it is the system of systems that makes the intellectual space challenging.

Accomplishing tasks with swarms of robotic agents is an emerging field with roots in computer science. These swarms are "a collection of (physical) agents moving in

[13] Exact image borrowed from: Austin, *Unmanned Aircraft Systems*, 9.

[14] Efron, *Unmanned Aerial Systems,* 17.

[15] Austin, *Unmanned Aircraft Systems*, 4–5.

real 2- or 3- dimensional space to fulfill certain mission requirements."[16] Swarms, or multi-agent dynamic systems, can accomplish tasks (missions) by following pre-established rules governing their geometries, formations, and methods. Gazi and Fidan point out that in multi-agent dynamic systems, the potential for emergent swarm properties, those that are greater than the individual physical pieces, is high.[17] Allen refines this premise, "Emergence is the manner of interaction of large numbers of entities and the patterns that arise from these interactions. The associated multiplicity makes the systems complicated enough that simple physics equations cannot accurately predict the 'emergent' system properties."[18] In computational simulation efforts, one may desire to design methodologies and rules which enable the agents to act in a way that creates these emergent properties. Conversely, regimented, centrally-controlled models, may have difficulty generating such characteristics.

B. AIRFIELD DEFENSE

Defending bases is not a new concept. Scores of studies, theses, governmental reports, and other publications all point to a need to defend key logistical and operational hubs.[19] However, these works focus almost entirely either on the systems and soldiers that work inside a base's perimeter, or on how the chain of command should work in forward operating locations. Ditlevson presents some information on UAS operations but only in reference to a single-entity platform and not swarms.[20] A few of Ditlevson's ideas appear to have been accepted as truth at the national-command level as the joint

16 Veysel Gazi and Baris Fidan, "Coordination and Control of Multi-agent Dynamic Systems: Models and Approaches," in *Swarm Robotics: SAB 2006 International Workshop: Revised Selected Papers*, edited by Erol Şahin, William M. Spears, and Alan F. T. Winfield, 71–102 (Berlin; New York: Springer, 2007), 72, https://link.springer.com.libproxy.nps.edu/chapter/10.1007/978-3-540-71541-2_6.

17 Gazi and Fidan, 73.

18 Theodore T. Allen, *Introduction to Discrete Event Simulation and Agent-based Modeling: Voting Systems, Health Care, Military, and Manufacturing* (London ; New York : Springer, 2011), 175.

19 See Vick (2015); Shlapak and Vick (1995); Schneider (1971); Penny, Hellgren, and Bessford (2013); Gray (2006); Ditlevson (2006); Covault (2009); Christensen (2007); Buonaugurio (2001).

20 Jeffery T. Ditlevson, "Air Base Defense: Different Times Call for Different Methods," (master's thesis, Naval Postgraduate School, 2006), 90–92.

publication authors incorporated them in some ways into the most recent Joint Publication (JP) 3–10, *Joint Security Operations in Theater*.[21]

JP 3–10 broadly aims to provide "guidelines to plan and execute operations to protect a joint security area (JSA)[22] outside the continental United States. Within [JP 3–10], these operations are referred to as joint security operations (JSO)."[23] The regulation goes on to discuss levels of threats to bases in three categories: single or few actors, small-scale (irregular warfare) forces, and significant (overwhelming) forces.[24] Understanding base defense in terms of these categories allows one to see what the Joint community believes an individual base is nominally supposed to be able to handle. In other words, the defensive footprint at a forward location must be able to deter and defeat single to small-scale forces on its own, and therefore should optimize itself to be superior against those types of forces. However, as asymmetric and sub-peer nations obtain more advanced weaponry, communications, and operational capabilities (night-vision, IR suppressants, etc.), the diverse list of potential threats to the air base continues to grow.

JP 3–10 calls for base commanders to pay particular attention to standoff weapons (mortars, missiles, other projectiles, and UASs).[25] The regulation warns, "Aircraft approach and departure corridors and the standoff weapons footprint immediately contiguous to air bases are elements of key terrain from which threats must be deterred and mitigated."[26] Unfortunately, many authors found base security doctrine and implementation to be lacking. Ditlevson echoes Shlapak, "USAF counters for the standoff threat are somewhat limited, and without a serious effort to detect standoff

---

21 Joint Staff, *Joint Publication 3–10 Joint Security Operations in Theater*, Joint Electronic Library (JEL), November 13, 2014, accessed February 12, 2017, http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.

22 "JSAs may be small or may span national boundaries, each with a distinct security environment and different policies and resources to address threats."—Joint Staff, *JP 3–10*, I-2.

23 Joint Staff, *JP 3–10*, I-1.

24 Joint Staff, *JP 3–10*, I-3—I-4.

25 Joint Staff, *JP 3–10*, I-2.

26 Joint Staff, *JP 3–10*, I-7.

attacks, high-value aircraft and other base operations could be jeopardized."[27] Vick adds, "The USAF has no organic ground-based defenses against aircraft; armed remotely piloted vehicle; or cruise-missile, ballistic-missile, rocket, artillery, or mortar attack."[28] Future analysis must address the specifics of that claim because Gray praises a joint Army/Air Force "integrated standalone security system (wireless mass notification systems, long range wide angle surveillance thermal imagers [with] infrared, ground surveillance radars, counter rocket, mortar technology)"[29] that is incorporated into the physical security measures for the base. Regardless of the base's interior technical capability, line-of-sight and logistic (including training and maintenance of expensive equipment) problems remain.

Buonaugurio believes that better, more effective, defensive posturing would occur if the Air Force returned to previous Security Forces Squadron manning levels, thereby supporting a largely defunct corps of tactical Emergency Services Teams (ESTs).[30] Additionally, he states that dispersal of high-value assets across multiple locations could assist defenders in the force protection problem. However, neither these solutions nor Vick's[31] are particularly suited to austere locations and they may be entirely impossible to implement due to funding or operational constraints. As the United States military continues to operate globally across the "spectrum of operations," it also requires a scalable, reconfigurable package that can operate in in a diverse set of conditions and provide defensive forces with emerging technology that can counter newer asymmetric tactics and threats. A UAV swarm could potentially support base defense in this manner, but one must analyze its abilities.

---

27 Ditlevson, "Air Base Defense," 7.

28 Alan Vick, *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*, (Santa Monica, CA: RAND Corporation, 2015), 39.

29 Ron Gray, "Integrated Swarming Operations for Air Base Defense Applications in Irregular Warfare" (master's thesis, Naval Postgraduate School, 2006), 59.

30 Michael P. Buonaugurio, "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision" (master's thesis, Marine Corps Command and Staff College, 2001), 32.

31 Conceal and Camouflage, Hardening, Dispersal—in Vick, *Air Base Attacks*, 40–54.

C. AGENT-BASED MODELING

A potential investigative method is to use Agent-Based Modeling (ABM) to create and optimize an algorithm for UAS swarms. Allen states that "Agent-based modeling involves the development of rules for individuals or entities and for the environment or background. The simulation proceeds as individuals execute their actions as allowed by the environment."[32] An ABM model (a computer program), essentially defines how certain actors interact with one another and the environment. Gazi and Fidan posit two types of models that are applicable to robotic swarms: higher-level and fully actuated.[33] The higher-level model (also known as a *kinematic* model) "ignores the lower-level vehicle dynamics of the individual agents (e.g., robots). However, it is a relevant and useful model since it can be used for studying higher level algorithms independent of the agent/vehicle dynamics and obtaining 'proof of concept' type results for swarm behavior."[34] In this effort, I aim at this "proof of concept" level, abstracting away from the details of physical mechanics, to focus on the problems of force posture and decision-making within an autonomous system of systems.

Since ABM is a relatively new field, there is a lack of literature on how to accurately model emergent properties in swarms.[35] Additionally, as there are no examples of UAS swarms in airfield defense roles,[36] evaluators must use multiple methods must to determine if it is best for swarms to operate autonomously/semi-autonomously and if a single program or "collective perception"[37] should govern actions. Schmickl, Möslinger, and Crailsheim assert that "swarm density"[38] is a critical element

---

[32] Allen, *Introduction to Discrete Event Simulation and Agent-based Modeling*, 177.

[33] Gazi and Fidan, "Coordination and Control of Multi-agent Dynamic Systems," 75–77.

[34] Gazi and Fidan, "Coordination and Control of Multi-agent Dynamic Systems," 76.

[35] Gazi and Fidan, "Coordination and Control of Multi-agent Dynamic Systems," 73.

[36] This author knows of no unclassified published examples of this type of research.

[37] Thomas Schmickl, Christoph Möslinger, and Karl Crailsheim, "Collective Perception in a Robot Swarm," in *Swarm Robotics: SAB 2006 International Workshop: Revised Selected Papers*, edited by Erol Şahin, William M. Spears, and Alan F.T. Winfield, 144–157 (Berlin ; New York: Springer, 2007), 144, https://link.springer.com.libproxy.nps.edu/chapter/10.1007/978-3-540-71541-2_10.

[38] Schmickl, Möslinger, and Crailsheim, "Collective Perception," 151.

in robotic swarms, though it is currently unknown what level that should be in defensive operations.

Lastly, the swarm itself, even if optimized, must either explicitly support existing structures and practices, or drive a complete shift in operations. Hubbard's research confirms this assertion; he found that while autonomous actors offer many advantages, warfighters will still "require that unmanned systems be interoperable on many levels, to include the ability to dynamically share information, including situational awareness and targeting information, with other unmanned systems and with manned platforms."[39] The swarm can conduct its own operations, but should support the base's overall defensive scheme.

Regardless of how the base-defense model changes, the UAS must still deconflict with traditional aircraft operations. This can be accomplished through scheduling (at the expense of effectiveness), lateral offset (potentially detrimental), or by onboard systems "such as traffic collision avoidance systems (TCAS) that are now used by human pilots on passenger aircraft."[40] However, with each added on-board system, an individual agent will carry less payload or it will suffer an endurance penalty due to the increased weight.

D. POTENTIAL ISSUES

Skeptics will point to, among others, ethical concerns, sustainability, or even a lack of technical capability. Ethically, some find UAV strikes to be appalling, "But sometimes imminent and intolerable threats do arise and drone strikes are the best way to eliminate them."[41] Concerns about autonomous UAVs conducting strikes are valid even with the benefit of advanced image matching. It is well within the realm of possibility either noncombatants could be targeted erroneously, or that enemies could determine

---

[39] Hubbard, Curtis W, "Base Defense at the Special Forces Forward Operating Base" (master's thesis, U.S. Army Command and General Staff College, 2002), 2.

[40] Gonzales, Dan and Sarah Harting, *Designing Unmanned Systems with Greater Autonomy: Using a Federated, Partially Open Systems Architecture Approach* (Santa Monica, CA: RAND Corporation, 2014), 49, http://www.rand.org/pubs/research_reports/RR626.html.

[41] Byman, Daniel L, "Why Drones Work: The Case for Washington's Weapon of Choice," June 17, 2013, Brookings, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice.

ways to increase their own survivability by subverting the autonomous system's judgment criteria. Therefore, initially, this type of system would likely best be used in remote locations which have fewer local civilians and strict rules about approaching the base.

Addressing sustainability, if swarms can help foster safer environments for air operations then they implicitly support the logistics of resupply. If the airbase is safer, more aircraft can arrive at greater frequencies. Advances in 3D printing, material engineering, and even nanotechnology also will continue to increase UAS life cycles and options for sustainability.[42] Emerging technological evidence indicates that swarm-based approaches are increasingly feasible. Researchers at major universities have created instances of successful swarming behaviors and some of those efforts are in unison with DOD efforts.[43] The Johns Hopkins University Applied Physics Laboratory demonstrated "UAVs [that] could take off and land autonomously and could swarm cooperatively to detect targets."[44] Additionally, from successes like the aerially-deployed Perdix swarm, one finds that a swarm of UAVs working with a "distributed brain,"[45] essentially shared repository of information, can be used to execute military missions. These examples point to the need for further study of the conditions for successful deployment of autonomous aerial systems.

---

[42] Maryse Penny, Tess Hellgren, and Matt Bassford, *Future Technology Landscapes: Insights, Analysis and Implications for Defence* (Santa Monica, CA: RAND Corporation, 2013), 96, http://www.rand.org/pubs/research_reports/RR478.html.

[43] Johns Hopkins, MIT, Georgia Tech, and NPS (author knowledge) all have demonstrated UAV swarm capability—Gonzales and Harting, *Designing Unmanned Systems*, 46–47.

[44] Gonzales and Harting, *Designing Unmanned Systems*, 46.

[45] Department of Defense, "Department of Defense Announces Successful Micro-Drone Demonstration," 9 Jan 2017, https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration.

III. MODEL

A. WHY AGENT-BASED MODELING?

ABM represents a particularly promising approach to tackle this problem. Macal and North argue that "the systems that we need to analyze and model are becoming more complex in terms of their interdependencies. Traditional modeling tools are no longer as applicable as they once were."[46] ABM allows one to create and mold the specific construct that matches the desired environment and actions. ABM provides a mechanism to define the exact actors, capabilities, environment, and types of interactions that a modeler knows will occur in the real world. However, an exact model which perfectly mirrors its actual counterpart is nearly impossible to create and therefore, one aims to use ABM to evaluate hypotheses about projected outcomes using quantitative data, gathered from the best-available models.

The principal pieces of ABM are the *agents*, or various types of agents, themselves. "The fundamental feature of an agent is the capability to make independent decisions. This requires agents to be active responders and planners rather than purely passive components."[47] In ABM, the model is, in essence, the result of a pairing of an environment and the agents, or actors, which work within it. These agents may exhibit completely autonomous behavior where they choose their own paths and react to stimuli, be semi-autonomous where some actions are self-decided and others are directed by a central authority, or may be controlled completely by that central controller. Each type of model has distinct advantages, but the true advantage is how closely the agents mimic the real-world behavior that is being modeled. The degree to which an agent's decision-making process and priorities match its real-world counterpart's adds to the realism and usefulness of ABM.

---

46 Charles M. Macal and Michael J. North, "Agent-Based Modeling and Simulation: ABMS examples," in *Proceedings of the 2008 Winter Simulation Conference* (2008): 103.

47 Macal and North, "Agent-Based Modeling and Simulation," 101.

Macal and North define 10 criteria if one needs to deliberate on whether to use an ABM approach to a problem.[48] The airbase defense problem meets all 10 premises. Of particular importance is their argument that ABM is appropriate for models that require decisions and behaviors, where actors interact with one another for finite periods of time, that have a spatial component that affects both actors and interactions, and that must be scalable.

The first few items are not complex. It is not difficult for one to imagine actors of any variety, and certainly not robots, making decisions based on known parameters. It follows that an interaction between two or more actors is merely a change in each distinct actor's "known parameters." That these interactions happen within a contextually-defined space is also logical. Therefore, what is left to understand about why this type of model is so appropriate for base defense concerns scaling.

A *base of operations*, while a common term in military parlance, is also quite vague. It could be something as little as a remote-observation post for a few soldiers, or a massive combined air-sea hub for major military missions. Thus, to say that "UAVs could support base defense" implies that the mission of UAVs, and the number of them, would be different given a different base, or in modeling terms, a new environment.

ABM's inherent adaptability to change and its scalability are therefore quite important to modeling in this highly variable domain. One can force the software to run the gamut of options to see what happens in a model given different values in key variables. Afterwards, one can, given a set of variables and corresponding outputs, conduct statistical analysis to determine if there are key elements, a particular value or relationship ratio between variables, or sequence of events, that indicate a higher probability of particular outcomes. That conclusion can help decision makers determine best courses of action or drive future changes in operating constructs or procedures. Additionally, modelers can run thousands of iterations testing the model under different circumstances testing the validity of premises and defensive algorithms. Then, if the

[48] Macal and North, "Agent-Based Modeling and Simulation," 110.

situation changes, one can simply recode the background environment while leaving all the high-level swarm interaction rules unchanged. The same swarm dynamics should, in principle, apply to any situation and the only changes one would need to make are to the environment variables and potentially some of the UAV's distinctive behaviors or decision-trees.

B. THE DEFENSIVE SWARM AGENT-BASED MODEL

1. Premise

To analyze how to best utilize the swarming UAVs, I developed a scenario along with associated computer algorithms[49] for swarm dispersion, patrol, investigation, and kinetic engagement in Python, an object-oriented programming (OOP) language with extensible libraries for ABM and performance analysis.[50] The model pits a swarm of defending UAVs against a variable set of enemies while recording the major interactions and outcomes that occur during execution. A user can run a model as a single instance and watch the interactions unfold, or create a batch process, where the computer runs multiple iterations with identical or altered settings without visualizing the model.

[49] Source code for all of my files is located in a NPS library repository; a basic explanation of the files is located in an Appendix at the end of this document.

[50] Python Software Foundation, "python," 2017, https://www.python.org/.

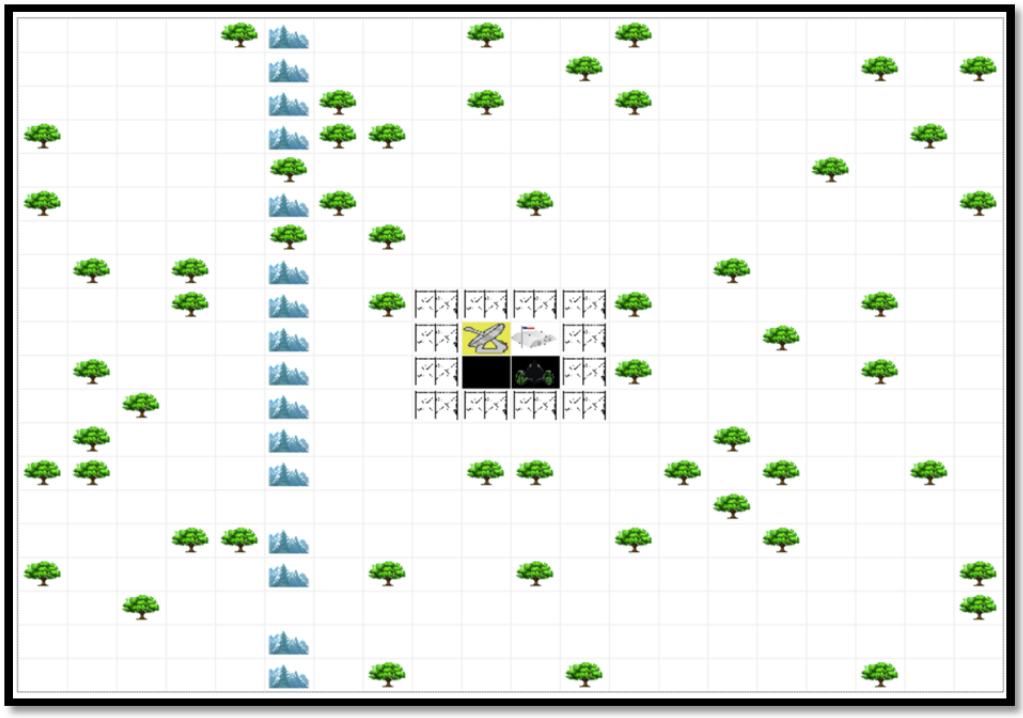


Figure 2. Defensive-Swarm Model Environment

The scenario in the Defensive-Swarm model focuses on a remote outpost that enemy militants are attempting to assault. The outpost, or base, is the primary focus for enemies and drones, which both have multiple types of agents. Enemies consist of mortar units, snipers, and UAVs. The defenders consist of UAVs, of which some or all may be armed with grenades, and the base itself. Visually, the computer depicts the environment, in a web-browser, as a grid. Each grid-square represents a 0.1 square-mile area, and one can set the model's size, its grid, to be any value between 30 and 300 (3–30 miles wide). To the left of the grid is a list of variables that the user can manipulate via sliders, drop-down menus, and toggle switches. These variables control important aspects like the number of drones, percentage of armed drones, which algorithms the defenders should use, and the numbers of enemies.

When a simulation is started, after a user chooses the parameters to be used in the model, the model's clock begins. In ABM, one method of controlling, and monitoring, the simulation is to have *time steps*. While the simulation represents continuous time, time steps are discrete portions of the overall period when the model updates (e.g., agents

move and interact) and the steps are sized to balance fidelity with overall efficiency in run-time. In these scenarios, the combat between enemies and drones is expected to be over in a matter of a few hours. Thus, each time step in the model is defined as a 15-second period (at step 40, 10 minutes of "real" time have passed).

During each step, the computer iterates through each agent in the model and gives it a *turn* to choose what to do. The enemies attempt to move closer to their firing positions by either taking the most direct or most concealed route (utilizing tree cover). Eventually, they will use their turns to attack the base. The defensive drones, conversely, spread out and search the area for enemies and engage them based on probabilistic chances of finding, identifying, and successfully targeting an enemy.

The parameters that a user chooses (swarm size, number of enemies, etc.) can drastically affect the outcome of the model. Therefore, in my testing, I ran the model using a batch process which creates, and evaluates, new instances of the model with different parameter values a set number of times. By checking a range of values on multiple occasions, I was able to examine whether the result values converged toward a standard outcome for a given scenario. This allowed for assessment of how a particular value may impact the probability of a certain type of outcome.

Whether one is running a batch or single instance, the model considers itself to be completed when all enemy agents have exhausted their available moves (they have been killed, escaped, or fired all their rounds). In batch processes, I limited this to 400 steps but with a world size of 7.5 miles, most trials only lasted into the high-200s to low-300s, or roughly 1.25 hours of real time. Of note, because the enemies always generate at the outer rim of the model, smaller-sized models invariably take less time to complete and larger ones take longer.

The base itself, always centered in the grid, is made up of four sections (squares): 2 runway/airfield operations pieces (large enough for some short-field aircraft and all U.S. Army rotary wing),[51] a housing piece, and a Command and Control (C2) block (a

[51] Department of the Army, *FM 3–21.38 Pathfinder Operations*, April 2006, 4–3, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm3_21x38.pdf.

headquarters, operations center). In the model, the mortars will target any of the base's pieces, but snipers will always target the housing or headquarters area. This does not change how the drones behave, but does impact the pathfinding that a sniper or mortar agent will use to navigate towards its target.

The entire base is surrounded by a fence which is meant to represent not only a physical fence, but some basic fortified positions from which the base's personnel can defend against enemies. Constructed in this way, the base covers about 0.4 square miles of land. While not as large as major forward-operating bases, which often feature significantly larger runways (often between 6000–12000 feet), the same principles of perimeter defense apply to larger bases. With a larger base, there could potentially be a penalty to drone loiter time due to the increased distance required to move outside the perimeter from the airfield. However, as the drone agents modeled are quad-copters, there is no requirement for them to have any sort of a runway. Indeed, were there to be UAVs assigned to a base-defense role, the logistic setup within the base itself would require careful research and analysis itself.

The surrounding area (white squares) simulates undulating, semi-prepared (rough) terrain which prevents unlimited line-of-sight (LOS) surveillance from the base. To add to the enemies' advantage, the tree squares represent small forests or clumps of trees where an enemy sniper is able to attempt to hide from the drones flying overhead. The mountains represent impassable trails that drones are also unable to overfly. Thus, they inhibit either side from moving through those particular areas.

2. Code Implementation

For this study, I implemented my code by extending the Mesa ABM framework[52] developed by Jackie Kazil and the Project Mesa team.[53] The developers state that Mesa "allows users to quickly create agent-based models using built-in core components (such as spatial grids and agent schedulers) or customized implementations; visualize them

[52] Source code repository for Mesa located on GitHub at: https://github.com/projectmesa/mesa.

[53] Mesa Team, "Mesa: Agent-based modeling in Python 3+," http://mesa.readthedocs.io/en/master/.

using a browser-based interface; and analyze their results using Python's data analysis tools."[54] Their software controls the basic structure of the user interface and the engine behind the model. One can think of it as a template where a programmer can pick and choose which pieces best work for a particular problem set. Within Mesa, there are different types of models and schedulers that one can use to create a simulation (e.g., models where all the actors move at the same time or where a type of actor always gets to move first). I chose Mesa due to its scalability, non-operating system specific visualization library, and because it appears to be the most actively developed ABM library in Python 3.

C. AGENTS

1. Operator

The Operator agent does not actually appear in the model but rather provides common functionality for both protagonists (Base, Command and Control, Defending UAV) and antagonists (Sniper, Mortar, Enemy UAV). All agents adopt the inherent capabilities of an Operator. Therefore, every agent (each an Operator) has a basic understanding of the model's grid (the simulated area's map), can identify that other agents are within a defined proximity (sharing a square), and understand route-traversal logic which allows them to create pathing solutions. Each agent is able to use this overarching logic to look for an optimal path toward a goal position. Additionally, an agent also knows its current position relative to a goal or other position. This mimics a real-world awareness of where one is relative to a target or objective.

2. Base

The Base agent represents the organic defensive capability at the remote base. It has an ability to detect an enemy UAV within 1000 meters at a probability of 75% via sensor.[55] The degradation in detection is modeled to allow for altered enemy drones that are operating outside of expected frequency bands or due to interference with the large

[54] Mesa Team, "Mesa: Agent-based modeling in Python 3+," http://mesa.readthedocs.io/en/master/.

[55] Drone Labs LLC, "How We Compare," 2017, http://dronedetector.com/compare-detection-systems.

numbers of friendly UAVs in the area. It will engage an Enemy UAV within its range at a probability of kill of 50%, simulating the difficulty of hitting a small target hovering hundreds of feet above a defending rifleman. The model gives ground enemies (sniper, mortar) the advantage of surprise in that the base's personnel will never identity a potential enemy (thus relying completely on drones for threat identification and engagement). Additionally, the base agent does not fight back against any attacking enemies, furthering the enemy's advantage. The following figure, and after each subsequent section describing an agent, shows the visual depiction of how the agent appears in the simulation.

Figure 3. Base (Barracks) Icon[56]

3. Command and Control (C2)

While each drone is responsible for its own search pattern, the C2 agent is the predominant brain of the defensive swarm. It creates and assigns the initial geometric dispersion (formation) of drones based on whether the user desires to have a threat-based or full-area algorithm. Under the threat-based algorithm, the drones will only patrol out to 0.8 miles beyond the maximum engagement distance for the enemies that are present in the model. Under the full-area algorithm, the drones will patrol the model's entire area. Once an area is set, smaller sectors are created for each drone to scan based on the number available. Essentially, the C2 unit divides up the defendable area into smaller

[56] Exact image from http://www.clipartpanda.com/clipart_images/clip-art-categories-60036150.

blocks and sets a patrol-distance limit for each individual drone (to eliminate excessive overlap and maintain coverage over the entire area).

The C2 agent tracks all available drones and receives reports from each of them when potential threats are discovered and when targets are engaged or terminated. The C2 element also tracks all reported threats and, each turn, checks its known-threat matrix against assigned assets. When there are many targets and fewer drones, the C2 element prioritizes its available fires against what it perceives to be the most lethal threat. In the model, snipers are considered the highest-priority, and then mortars, because a mortar round can be "stopped" by a small team of drones hovering over the tube (at a 100% loss to the drones overhead), while snipers can only be stopped by kinetic strikes. The C2 agent assigns the lowest priority to enemy UAVs as these units have no ability to directly damage the base.

In general, the C2 agent looks for the closest available drone to support any tracking or targeting missions. Until assigned to a target, each drone is responsible for its own scan pattern and decision-making. Once assigned, the drone begins moving towards the target and switches its behavior from a patrol logic to either investigating or attacking.

Figure 4. C2 Icon[57]

[57] Exact image from https://publicdomainvectors.org/en/free-clipart/Satellite-dish-vector-clip-art/9878.html.

4. Defensive UAV

These UAVs are the primary defensive force in the model. They operate exclusively external to the base and do not support operations inside the base's perimeter. In this simulation, all drones have an optical capability (high-definition video camera), a transmit and receive antenna, and optionally, two grenades for target engagement. In this model, drone kinematics are roughly based on the capabilities of a DJI Phantom 4.[58] The Phantom 4 is able to climb at 20 feet per second, descend at 13 feet per second, move at 66 feet per second, has a maximum flight time of 28 minutes, and can achieve a maximum altitude of 19,685 feet.[59] The major difference in the batch-simulation models is that the drones were allowed a one-hour flight time, after which they had to return to the base. This decision was made in order to test the effectiveness of the initial dispersion and search algorithms, without the added complication of unit replacements to ensure formation integrity. If successful, future research could focus on the question of how best to maintain the persistent presence (drone formation).

Every time-step for a drone on patrol simulates covering 0.1 square miles (278,784 square feet). The presumptive scan pattern takes approximately 11 seconds to fly (at 50 feet per second) at an altitude of 200–300 feet (observing a 360 foot by 240 foot area with its field of view). Processing of images is assumed to be accomplished onboard each drone, but in the future could be assisted by a neural network as part of the C2 element.[60] The unit moves to the next area during the final 4 seconds of each step. The drone's optical capability includes full-motion video and analysts report that acquisition

---

[58] DJI, "Phantom 4," 2017, https://www.dji.com/phantom-4.

[59] DJI, "Phantom 4 Specs," 2017, http://www.dji.com/phantom-4/info#specs.

[60] Jangwon Lee, Jingya Wang, David Crandall, Selma Šabanović, and Geoffrey Fox, "Real-Time, Cloud-Based Object Detection for Unmanned Aerial Vehicles." Extracted from *2017 First IEEE International Conference on Robotic Computing (IRC),* (Taichung, 2017), 6, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7926512&isnumber=7926477; Additionally, see sample recognition capabilities by Vicomtech-IK4, "Real Time Detection of Events for Surveillance Applications," 2013, http://www.viulib.org/solutions/s24/real_time_detection_of_events_for_surveillance_applications.

of a person requires the drone maintain "line-of-sight to the target at a range of less than 500 meters, but often much closer distances (about 100–200 meters)."[61] At planned altitudes, the drone should be able to discern human characters or other threats. A defending UAV can identify mortar and enemy UAVs immediately. For snipers, the drone tracks the unit until it determines that the person it is following is indeed hostile (observes the sniper attack, identifies the figure as a sniper[62]). Upon that realization, it alerts C2 of the new threat.

While in its "patrol" logic, a drone chooses its next move by checking the "neighborhood" of locations (0.1 miles in any direction, but it may not choose its current position) into which it can move. Internally, the drone eliminates a square from consideration if it is beyond its individual patrol distance, is beyond the necessary search area (usually set to 0.8 miles beyond the maximum threat's range), or is an invalid position (e.g., overhead the base or a mountain). Once the drone establishes a list of potential moves, it pings the C2 unit to get a list of the most recently visited (searched) areas. Then it chooses the least recently searched part of its neighborhood and reports its decision to the C2 unit.

"Seeker" (purely ISR) drones and "Bomber" drones behave identically, except that bomber drones can launch up to two direct kinetic strikes to destroy ground-based enemy units. As this is a *higher-level* model, the specifics of how a drone turns, hovers, or physically performs actions is not analyzed. The model assumes that a drone can takeoff, land, move to locations, and conduct strikes. The specifics of exactly how a drone tilts its rotors or positions itself are not considered. Instead, the model focuses on the drone's operational mission. Additionally, the model also sets six minutes as the time

---

[61] E. Peters, Somi Seong, Aimee Bower, Harun Dogo, Aaron L. Martin and Christopher G. Pernin, *Unmanned Aircraft Systems for Logistics Applications* (Santa Monica, CA: RAND Corporation, 2011), 52, https://www.rand.org/pubs/monographs/MG978.html.

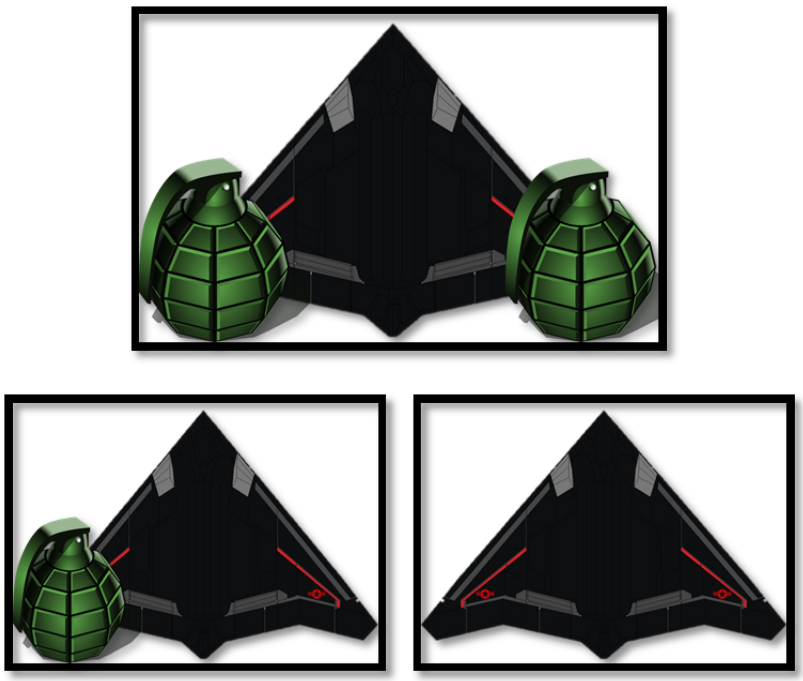
[62] This behavior simulates that the defending UAV has the ability to compare its images with a database of images or templates to appropriately identify the target.

it takes the base's personnel to replace a battery and rearm a drone to full operating capacity. It assumes drone batteries all provide the exact same loiter time with no variation. Finally, the model assumes that, kinematically, a drone sub-swarm can hover perfectly over a mortar tube such that if a round impacts a set of four drones, it will detonate.

Allowable numbers of agent: 10 to 300
Range (of detection and engagement): 0.1 miles
Movement: 45 miles per hour
Capabilities: Block a mortar shot; collide with and damage or destroy Enemy UAV (one collision to destroy an Enemy UAV)
Battery Depletion Rate: 1 unit every 15 seconds

Figure 5. Defensive UAV ("Seeker") Icon[63]

[63] Exact image from http://bestairdrone.net/horizon-hobby-blade-nano-qx-rtf-quadcopter/.



Allowable numbers of agent: 10 to 300
Range (of detection and engagement): 0.1 miles
Movement: 45 miles per hour
Capabilities: Kinetic strike against ground units; collide with Enemy UAV (only if 0 grenades)
Battery Depletion Rate: 1 plus 0.1 units per grenade (drag/weight penalty) every 15 seconds

Figure 6. Defensive UAV ("Bomber") Icons[64]

5. Enemy

The Enemy type is essentially just a shell for the subsequent sub-varieties (Sniper, Mortar, and UAV). Similar to Operator, the Enemy agent definition provides common functionality to the antagonist types, including turn logic (what each agent should do on its turn), ingress logic to a firing position, and path-finding based on avoiding opponents and returning to its origin (only used by Snipers).

[64] Exact image of bomber graphic from https://bagera3005.deviantart.com/art/Lockheed-EA-22b-Eraser-198837080; Exact image of grenade clipart from http://www.clker.com/clipart-grenade-2.html, combination of graphics by author.

6. Sniper

The Sniper type emulates a real-world sniper (or team) that moves into a position, shoots at the base's defenders and then egresses to safety once out of ammunition (50 rounds, at 5 shots per time step). The Sniper does not ever try to get closer to base than necessary to take its shot. Additionally, its movement logic favors the utilization of environmental protection (e.g., going through trees instead of the open field) to minimize detection. Snipers are different than Mortars in that their visibility to drones is masked by 66%. A RAND report suggests drones can detect about one-third of threats like snipers using real-time sensors;[65] this report addressed fixed positions but the concept is applied here to simulate the intrinsic ability of a sniper to hide himself from his opponents. The model assumes that there is some level of cover even in the open area, but if a sniper is able to maneuver through trees, his likelihood of detection drops to zero while in cover (once discovered, the model presumes that the multiple seekers will be able to maintain visibility on a target). A sniper will die if one Bomber UAV conducts a single successful strike against him.

[65] E. Peters, Somi Seong, Aimee Bower, Harun Dogo, Aaron L. Martin and Christopher G. Pernin, *Unmanned Aircraft Systems for Logistics Applications* (Santa Monica, CA: RAND Corporation, 2011), 20, https://www.rand.org/pubs/monographs/MG978.html.

Allowable numbers of agent: 0 to 50
Range: 0.4 miles (~ 400 meters)
Movement: 4 miles per hour over semi-improved terrain on foot
Capabilities: Damage base
Survivability: Killed by a single grenade

Figure 7. Sniper Icon[66]

7. Mortar

Mortars simulate a real-world team of personnel moving a mortar into position, via vehicle, to take a time-delayed shot. In the model, the mortar team moves as quickly as possible into position and sets the mortar. After 10 minutes, the mortar fires regardless of whether it has been discovered or not by drones. This time simulates allowing the mortar team (adversaries) to leave the premises and either trigger a remote engagement, or allow a timer to expire. If the drones discover the mortar before it fires, and assemble a sub-swarm above the mortar, the shot is blocked by defenders. Here, the simulation presumes that the mortar round is on an impact-fuse and will detonate upon striking the swarm of drones hovering above its muzzle.

The mortar is based on the 2B-14 Podnos 82-millimeter mortar, which has a maximum range of 4,000 meters (~2.5 miles).[67] In this simulation, the mortar fires a single shot and there is no ability for enemies to resupply or reuse them. For the

[66] Image from http://www.iconsplace.com/search/sniper+rifle-black, recolored by author.

[67] Jane's Defence Equipment & Technology Intelligence Centre, "2B14 Podnos 82 mm light mortar," Jane's by IHS Markit, 2017, https://janes.ihs.com.libproxy.nps.edu/Janes/Display/jiw_0909-jiw.

defenders to defeat the mortar, requires 3 successful grenade strikes. While a high-explosive grenade is not likely to damage the hardened muzzle, the blast or damage to the terrain near the mortar's legs should knock it over, or at least off target.

Allowable numbers of agent: 0 to 50
Range: 2.5 miles
Movement: 12 miles per hour over semi-improved terrain[68]
Capabilities: Damage base
Survivability: Killed by 3 grenade strikes

Figure 8. Mortar Icon[69]

8. Enemy UAV

An Enemy UAV provides intelligence to the adversaries. Once the UAV launches, it flies in the most direct route toward its target and loiters over the base, simulating that it is collecting intelligence and camera footage that would support the sniper and mortar attacks. In this model, however, since the snipers and mortars attack with a 100% accuracy rate (to consistently penalize a failed defense), UAV intelligence has no impact on the ground attackers' capabilities. While the UAVs themselves do not physically attack the base, they do draw seekers away from their positions. As the seekers attempt to attack inbound UAVs, their presence can detract from the integrity of the

[68] John E. Peters, Somi Seong, Aimee Bower, Harun Dogo, Aaron L. Martin and Christopher G. Pernin, *Unmanned Aircraft Systems for Logistics Applications* (Santa Monica, CA: RAND Corporation, 2011), 54, https://www.rand.org/pubs/monographs/MG978.html.

[69] Image from http://www.iconsplace.com/search/mortar-black, recolored by author.

defensive formation either temporarily or permanently (any collision destroys both the enemy and defending UAVs). In future models, UAVs could carry their own armament to attack the base or its personnel, attack defending drones, or increase the accuracy of remaining (future) enemy attacks.

Allowable numbers of agent: 0 to 50
Range (of observation): 0.1 miles (per 15 seconds)
Movement: 30 miles per hour
Survivability: Killed by 1 collision with a Defensive UAV or by the base's personnel

Figure 9. Enemy UAV Icon[70]

9. Tree and Mountain

Trees and mountains provide cover and obstacles to the other mobile agents. While feasible that a DJI Phantom 4 could vertically clear most any mountain, the time it would take to climb above a large obstacle and descend to the opposite side would render its loiter time to fractions (if any) of its potential. Additionally, the signal interference imposed by having a mountain in between the drone and its C2 would likely result in zero connectivity.

[70] Image adapted from http://clipground.com/quadrocopter-clipart.html/, recolored by author.

Figure 10. Tree Icon[71]

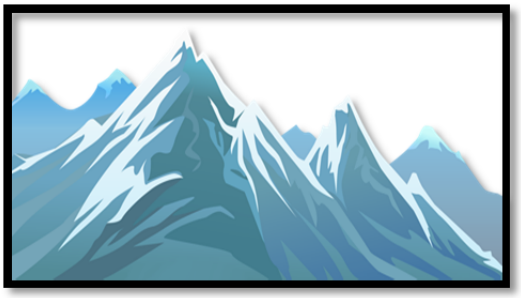


Figure 11. Mountain Icon[72]

D. MODELING DECISIONS

In creating a model like this, one could focus on a singular threat or strive to include every variation of weapons and tactics that enemies use to target a base. In order to work towards a "proof of concept," I chose to limit the number of threats and types of actions to focus attention on variation in the control-logic used by the central arbiter (the C2 agent). In limiting the number of threats, I also limit the simulation to be one overall contest such that no external forces exist that can assist either side in the conflict. There are no reinforcements available to either side with the exception that Defensive UAVs are able to return to base to refuel and rearm.

---

[71] Exact image from http://cliparting.com/free-tree-clipart-1214/.

[72] Exact image from https://gallery.yopriceville.com/Free-Clipart-Pictures/Winter-PNG/Snowy_Mountain_Transparent_PNG_Clip_Art_Image#.WhySlkqnHt8.

1. System Dynamics

The defensive-logic system for a drone is a series of behaviors that switch based on interactions with or inputs from other actors, or from its own internal status. A drone will generally stay in its patrol behavior unless it encounters an enemy actor, is ordered to a different function by the C2 element, or hits its "bingo"[73] point and is forced to return to base (RTB) to get a new battery. Bombers will do the same except that they have the added logic of potentially returning to base if they are out of grenades and not currently tasked to an investigation mission.

Once a drone finds a human target, it passes the position of the target to C2 along with an "unknown" status of whether it is a threat or not (e.g., not yet know whether it is a sniper, or just a person hiking in the hills). If the drone finds an object which it determines to be a threat immediately, as is the case with a mortar and enemy UAV (these objects have no non-threatening reason to be near the base), then in its initial alert to C2 it also reports that its object is a threat. Depending on the message, the C2 element will task drones to investigate (observe and track the target), or attack (which also entails an investigative sub-swarm to assist with tracking or blocking, in the case of the mortar). Table 1 lists the C2's desired sub-swarm sizes, which are contingent on the type of enemy.

Table 1. Desired Sub-swarm Sizes

Enemy	Track	Target
Mortar	4	3
Sniper	2	2
UAV	1	

[73] A term used in military aviation meaning that there is not enough fuel to continue the mission and that it is time to return to base. In this model, a drone will return to base and plan to land with just over a minute of battery life left.

After tasking a sub-swarm, the C2 element continues to reevaluate its tracking and targeting matrices. A sub-swarm will continue to track a person (sniper) and once the swarm declares it as hostile to the C2 element, the C2 arbiter dispatches a bomber force to target the enemy. For targeting prioritization, in each time step (and after every engagement), the C2 agent checks its known-untargeted enemies list to see if a higher-priority target should be attacked. If a higher priority targets exists, or if a like-priority target has no bombers assigned to it and another has more than enough to kill the assigned target, it will reallocate the closest drone (from the target with multiple bombers) to address the untargeted enemy. This prioritization function (further refined in Figure 12) is one of the most important pieces of artificial intelligence decision-making in the model and it is especially important to the defenders in simulations that have fewer bombers available as it minimizes the number of assets the C2 agent assigns to each target.

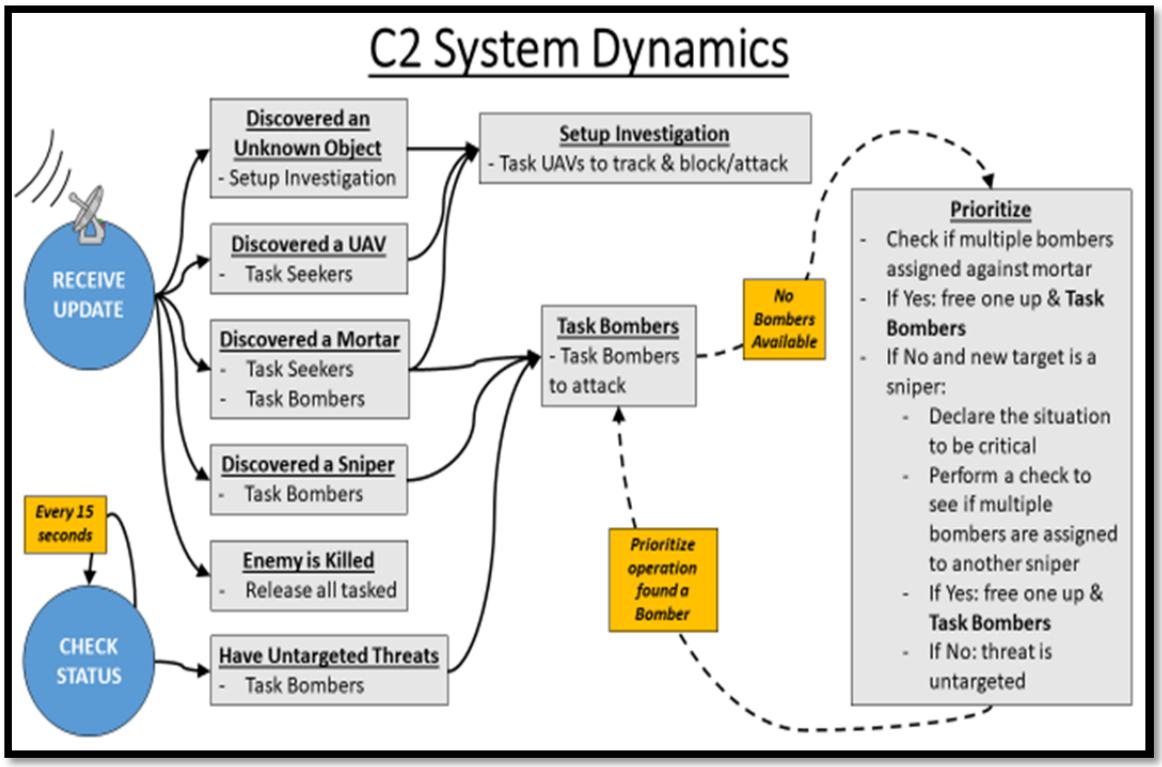
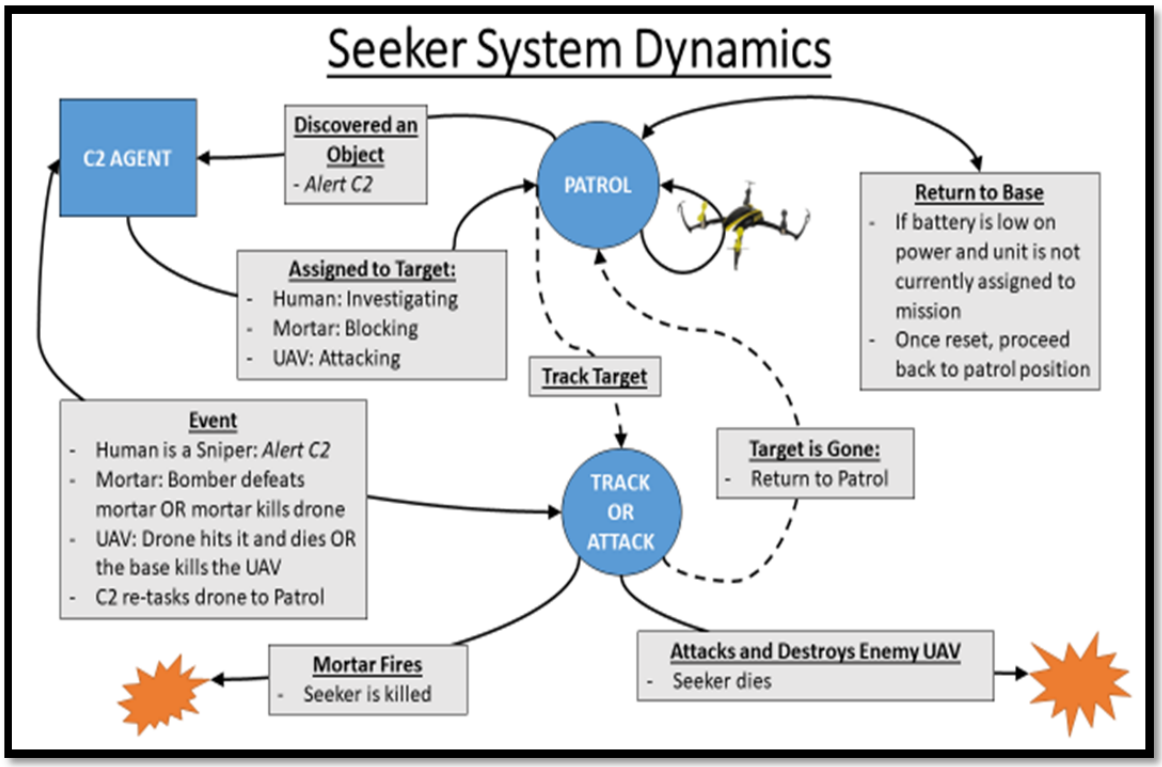


Figure 12. C2 System-Dynamics Diagram

Once a target is eliminated, all forces assigned to it are released back to their patrol points. The exception is when drones have been killed by either attacking an enemy UAV (crashing into it) or by mortar fire. Those drones are lost and no new drones are launched from the base to replace the missing members. Bombers with no remaining grenades request to RTB to rearm and seekers invariably move back to their patrol points. Pictorial representations of the seeker and bomber system dynamics are in Figures 13 and 14, respectively.



Note that the C2 agent will select bombers with no armament remaining if there are no seekers available to support tracking or Enemy UAV engagement. Otherwise, that bomber will return to base, rearm, and follow Bomber System Dynamics (next figure).

Figure 13. Seeker System-Dynamics Diagram

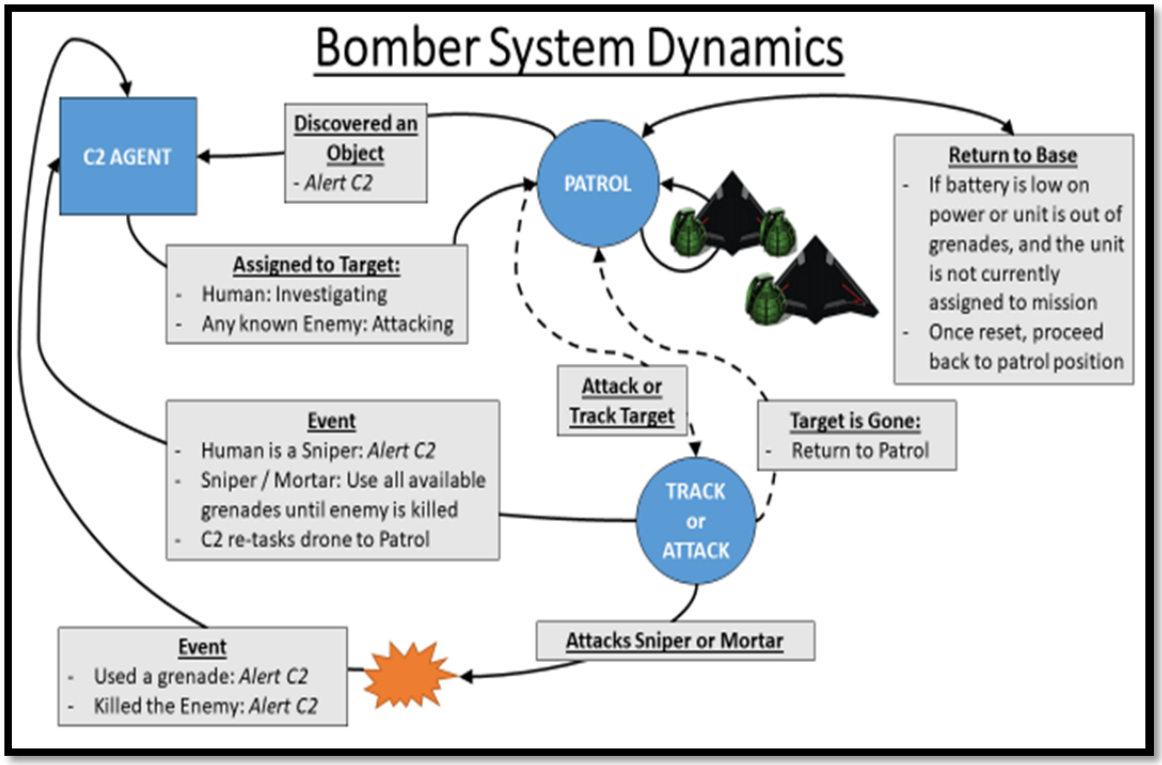


Figure 14. Bomber System-Dynamics Diagram

2. Variables

In the model, there are a number of system- and user-defined variables. The major system variables define agent capabilities and the coefficients that govern the likelihood of agent interactions, visibility, or probability of detection. The user-defined variables are all available to see upon launching a new instance of the model. These parameters shape the overall number of actors in a model as well as the defensive scheme that a user wishes to test. Changing any of these variables can have a substantive effect on the model's outcome. This is desirable because in different environments, in defenses against different types of enemies, or upon the advent of new drone technology, one would need to update the model to more accurately reflect the situation at hand.

a. System Defined (Actor—Variable)

(1) *C2—Bombers Required*: Controls how many bombers the C2 agent believes are necessary to engage a particular target. This provides additional grenades to target each enemy should an attack miss. In the model, this is set to two for snipers and three for mortars.

(2) *C2—Offset*: The amount of extra distance beyond the maximum threat range that drones should patrol. In the model, this value is set to 0.8 miles.

(3) *Defending UAV—Patrol Distance*: A value set by the C2 agent to inform a drone of how far from its patrol point it should be willing to stray during patrol. This allows each drone to have its own operating space with some minor overlap. This value is dynamic and is dependent on the type of patrol algorithm and how many drones are available for defense at a given time.

(4) *Defending UAV—Probability of Detecting a Person*: The probability (set to 95%) of detecting a person (sniper) when it is not hiding in terrain (trees). This does not imply that there is a 95% chance of finding a sniper if a drone is in the same location, but rather interacts with the sniper's ability to mask himself from a drone to determine the outcome. This value indicates the chance that a drone would find a human figure during its scan of an area and allots a 5% chance of error to that likelihood.

(5) *Defending UAV—Probability of Identifying a Sniper (prior to attack)*: The probability of a drone matching the person it is tracking to a "sniper template" in its database before the sniper begins shooting (set to 65%). Once a sniper begins to attack, a Defending UAV always recognizes the actor as a threat.

(6) *Defending UAV (Bomber)—Probability of Attack (Success)*: The probability that a bombing attack will succeed in striking the opponent (90% against mortars and 60% against snipers). This reflects the presumption that a mortar emplacement is a stationary target which enables the bomber to be able to descend to an effective altitude and engage. A sniper, alternatively, has greater ability to maneuver.

b. User Defined (Actor-Variable)

(1) *Patrol Algorithm—Random*: All drones start from the runway and move randomly in any direction and all drones (both types) are available for assignment. On each turn, a drone will continue to choose its next position randomly regardless of its position relative to other drones or the base.

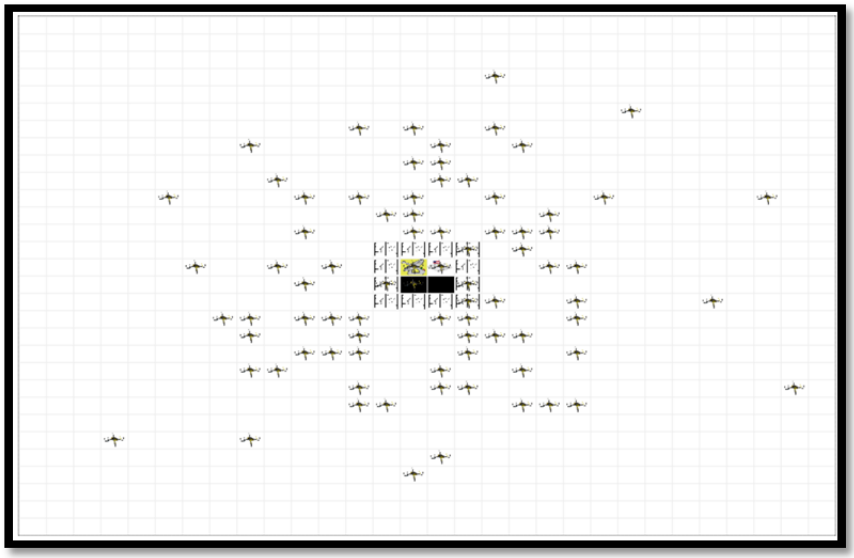
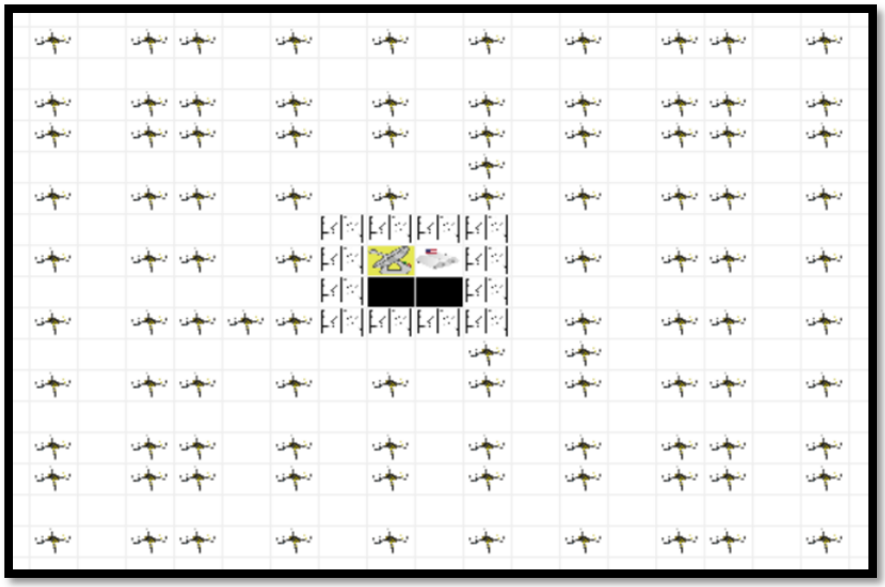


Figure 15. Random Patrol

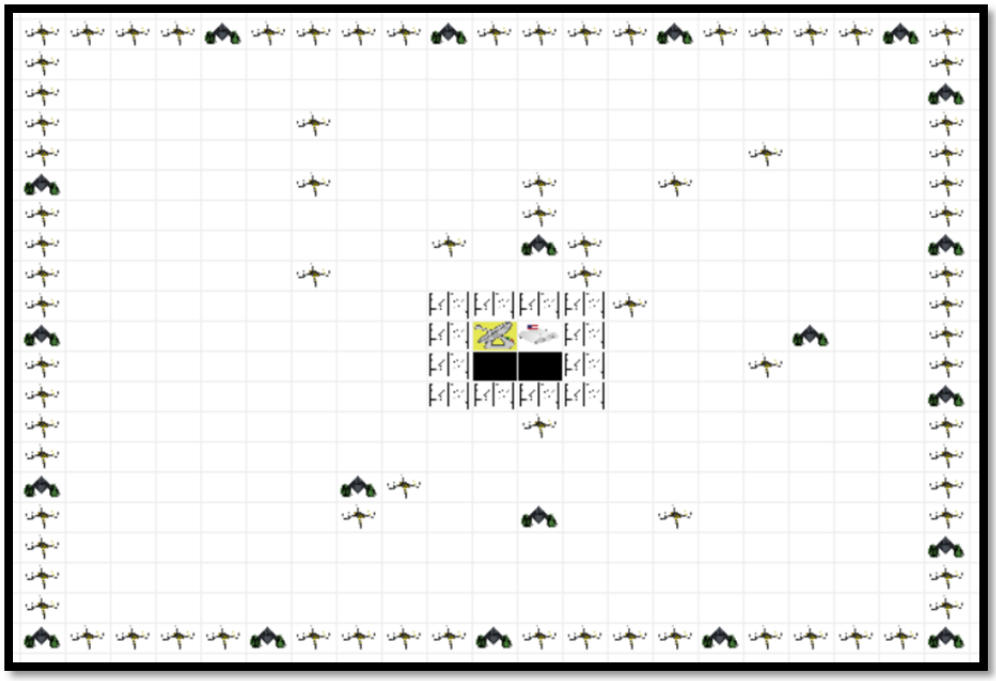
(2) *Patrol Algorithm—Grid*: The drones are dispersed in a grid format. They protect individual sectors and are all available for C2 assignments. If there are excessive drones that do not fit evenly into the spacing algorithm or would be assigned to patrol on top of the base, they are placed randomly near the base's perimeter to support close-in defense.



Drones are in position after launching from the runway and moving to their assigned locations.

Figure 16. Grid Patrol

(3) *Patrol Algorithm—Passive*: The drones create the largest box (it appears rectangular because the grid boxes themselves are not actually square) around the base that they can using 90% of the available assets (C2 agent reserves 10% of available drones inside the perimeter for additional threat tracking and engagement). The reserved drones operate within the ring and will stay close to the base in attempt to minimize the distance they may have to travel to support any taskings.



Perimeter drones will remain stationary until interacting with an enemy while interior drones scan inside the perimeter.

Figure 17. Passive Patrol/Defense

(4) *Threat-Based Defense* (ON/OFF switch): An attribute used by the C2 element to decide whether to use the maximum range of the threats present in the model when determining the maximum patrol distance for the drones. If "OFF," the drones will patrol the entire operating area.

(5) *Bombers Airborne Before Threat* (ON/OFF switch): This switch provides the user the ability to decide whether the defending swarm is authorized to operate in an armed configuration prior to discovering any threats to the base. If "OFF," every bomber will remain on the runway in a ready state waiting for a tasking.

(6) *Bomber Algorithm—Dispersed*: The bombers are dispersed evenly throughout the formation, in accordance with the user-prescribed bomber

percentage. This algorithm represents a potential dispersion plan which could be used in situations where it may be necessary to have bombers farther away from the base to stop enemies with long-range weapons.

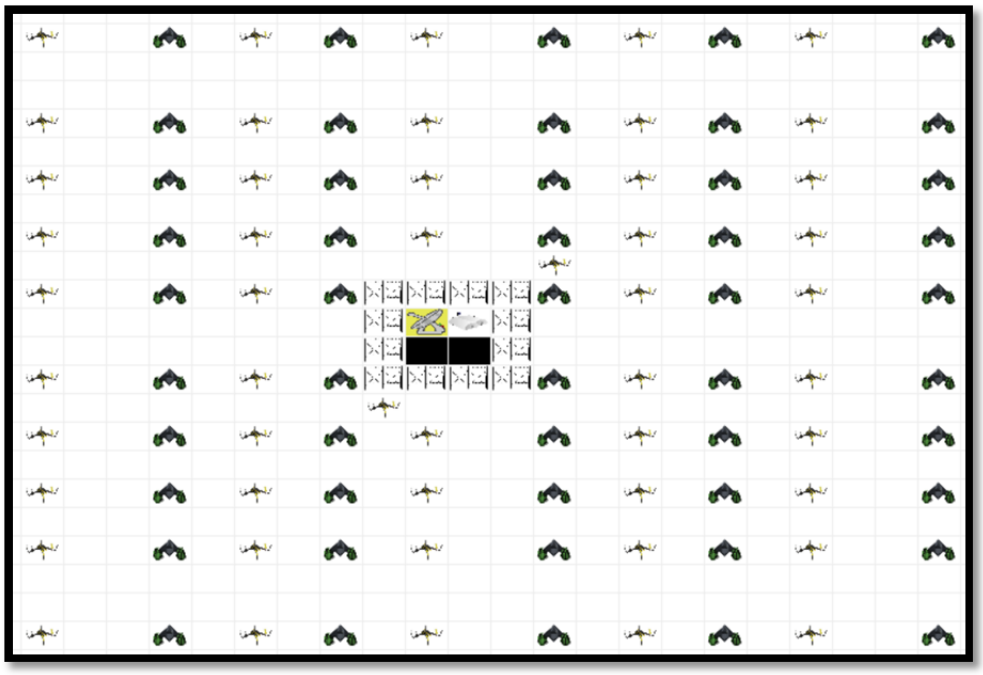


Figure 18. Dispersed Bombers

(7) *Bomber Algorithm—Centered*: The centered bomber algorithm focuses on keeping the bombers within a perimeter made up of seekers. As the user increases the percentage of bombers, more bombers will begin to appear along the periphery of the formation. This algorithm represents a potential dispersion which could be used in situations in which it may be better to have the bombing capability closer to the base itself to stop imminent threats.

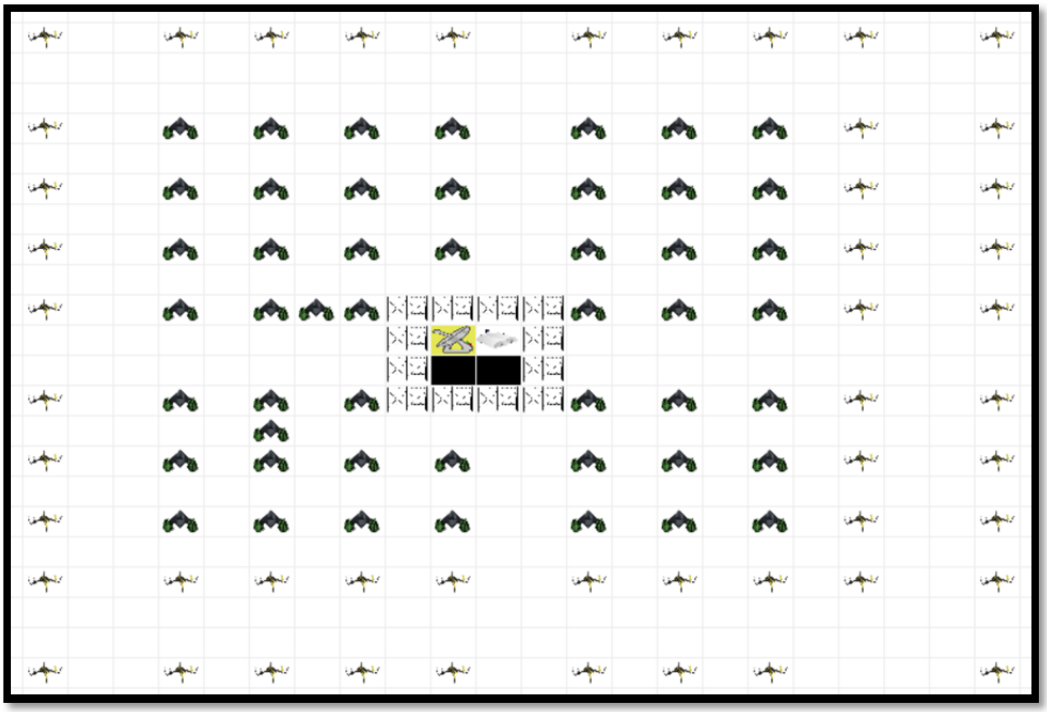


Figure 19. Centered Bombers

(8) *Time Before Enemies Appear* (0–100 steps): This slide bar allows the user to define how many steps the drones should get to setup before the enemies spawn and begin their approach to the base. Depending on the model's size, this value could be especially important because of the mortar's relatively long range. If the enemies are allowed to advance immediately, it may result in mortars firing before drones are able to discover and engage or block them.

3. Measures of Effectiveness

To determine the success or failure of a defensive formation, I needed measures of effectiveness. In this model, I graded the defending UAVs on the following parameters:

(1) *Average Time of Discovery*: The average number of time steps before a drone began tracking an enemy compared to when it could have been found (drones are not penalized for not finding an enemy that is on the grid but beyond the search perimeter).

(2) *Average Time to Eliminate*: Once discovered, the average number of time steps required to then eliminate the threat.

(3) *Unique Sniper Attacks*: The number of unique snipers that were able to ingress and attack the base.

(4) *Unique Mortar Attacks:* The number of unique mortars that were able to fire and damage the base.

(5) *Successful Attacks*: The raw total number of attacks that enemies were able to successfully launch against the base. If a sniper is able to accomplish multiple attacks, I add each one to this total.

(6) *Blocked-Attack Percentage*: The proportion of attacks stopped relative to the total number of *Successful Attacks*.

(7) *Enemies Stopped*: The total number of enemy units that that the swarm prevented from making any successful attack on the base.

(8) *Enemies*-Stopped *Percentage*: The total number of *Enemies Stopped* relative to the total number of enemies in the model.

Each measure has its own importance; but the overwhelming objective for the drones is to stop attacks. Therefore, while all metrics have their own merit and relay some understanding about the effectiveness of a particular swarm size or algorithm, the ultimate goal is to protect the base and its personnel while developing a method to minimize the need for forces to go "outside the wire" to patrol the surrounding area. Therefore, though the *blocked-attacks percentage* metric is the truest measure of a successful defense, the *enemies-stopped percentage* value is also used to evaluate the swarm so as not to overly weight the success of a single sniper (capable of multiple "successful" attacks by itself) relative to the whole of the defense.

IV. ANALYSIS

A. INITIAL ALGORITHM (SINGLE-RUN) TESTING

Prior to running any batch jobs, I tested each algorithm to observe drone behavior and search for positive and negative aspects in the various defensive postures (algorithm combinations). Initial testing focused on identifying errors in drone dispersion (the C2 process of setting up the initial positions for the swarm based on the patrol algorithm), determining appropriate model sizes, viewing interactive patterns of drones, ensuring the C2 element was appropriately reassigning bombers as new threats emerged, and checking enemy infiltration and exfiltration (for snipers) mechanics. Finally, the single-run tests helped me to eliminate the need for high-iteration batch analysis on a few of the algorithms, as I noticed some faults in operational application.

1. Patrol Algorithm—Passive

This plan did not survive first contact with the enemy. The Passive algorithm, in its current definition, was ineffective in almost every trial. The two primary issues with this defensive setup were that smaller swarms were not able to generate a large enough perimeter to stop mortars, and larger perimeters were prone to breaches, especially by snipers.

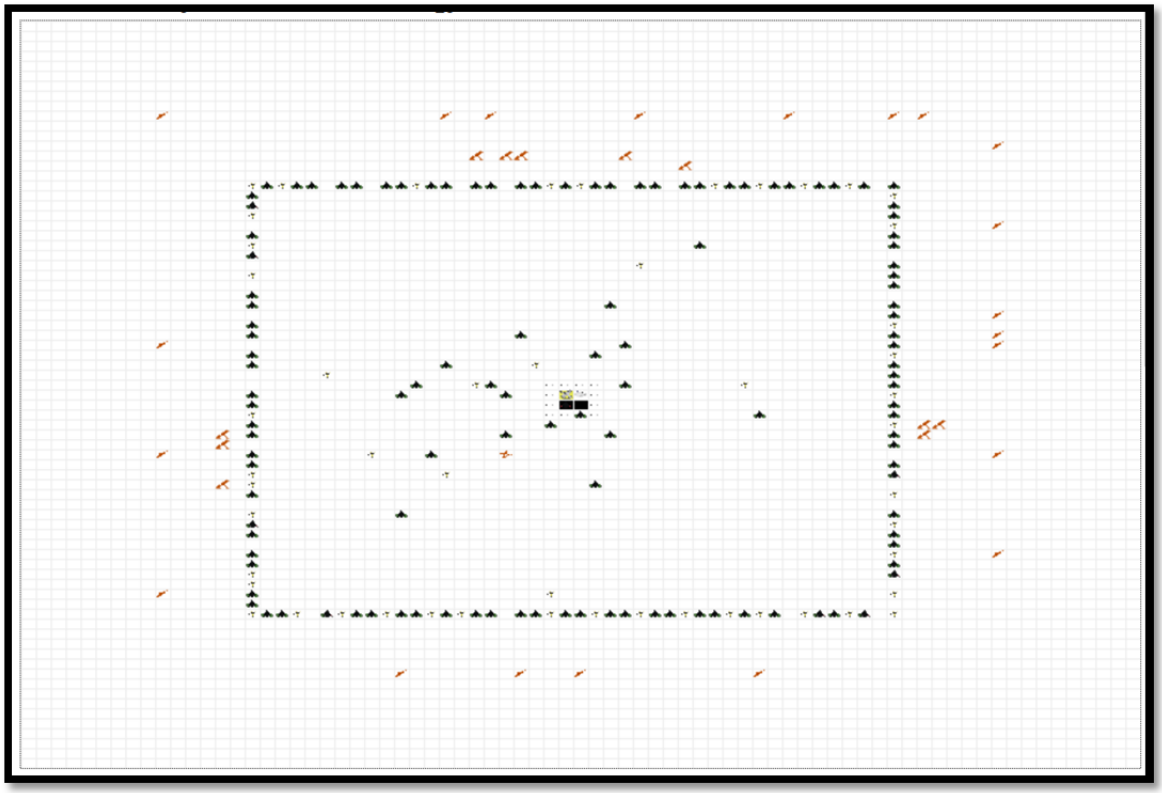
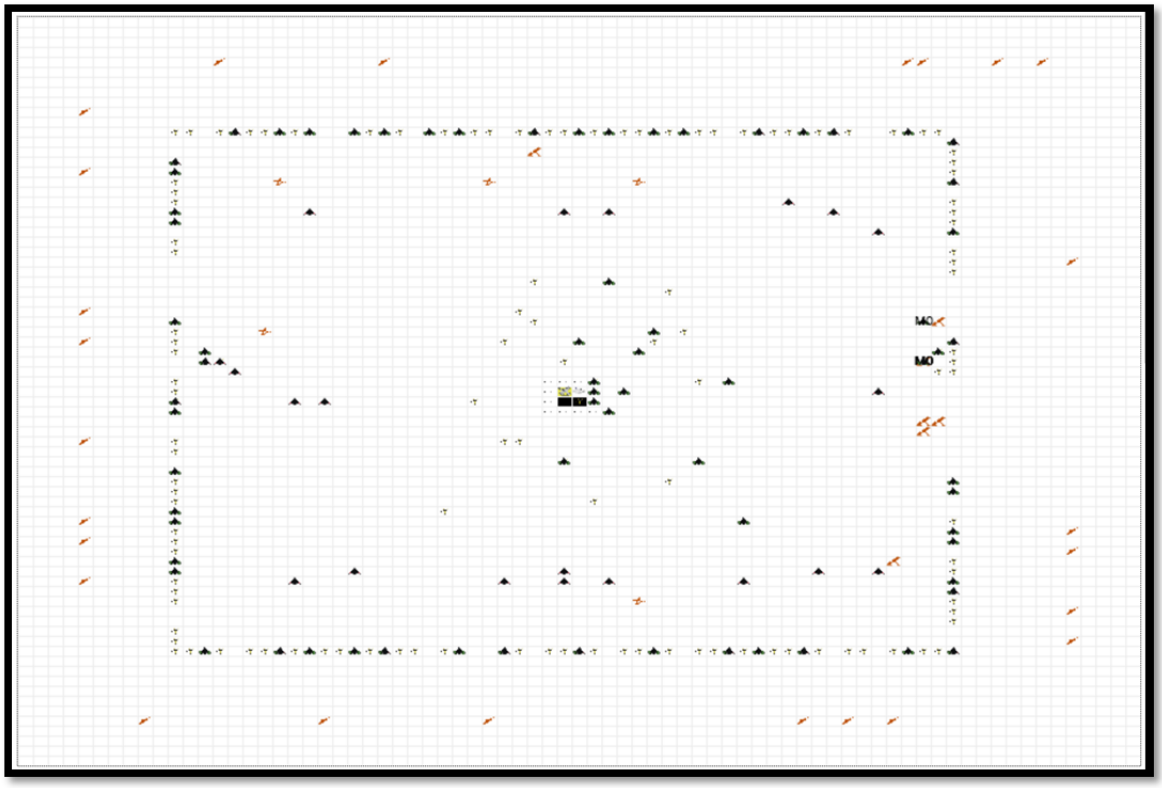


Figure 20. Mortars Preparing to Fire from Outside the Perimeter

The first issue is a major problem. While small swarms were generally ineffective regardless of the algorithm, the passive box had a distinct shortcoming in that there was no chance that a drone could intercept a mortar prior to firing because the box was generated well inside the mortar's maximum shot distance. This alone proved fatal to the algorithm's effectiveness, but additional detractors are worth mentioning in order to document improvements modelers should make in future developments.

Snipers were able to move through the line fairly effectively because of their ability to mask themselves from drones. If a sniper was not discovered by the drone guarding the space he moved through, then it was unlikely that he would be discovered by the reserve drones (the 10% operating inside the perimeter) prior to attacking. In smaller swarms, there was too little time to discover the sniper once through the line whereas in larger ones, the area inside the perimeter was too great to be effectively covered by the remaining 10%.



Note the four untargeted mortars able to ingress through the perimeter in the east because other defending UAVs are tracking and targeting other mortars. Without sufficiently high-percentages of bombers, the drones operating in this type of algorithm were susceptible to this behavior.

Figure 21. Passive Box after Penetration

Aside from their ability to sneak through, snipers also benefited heavily from the presence of UAVs or mortars. Both of those actors, faster than snipers, drew sub-swarms for tracking and engagement, which created holes in the perimeter. If the seekers were killed by either collision with an enemy UAV or from mortar fire, the hole became permanent and snipers could pass through with no chance of detection.

Due to its numerous shortcomings, I elected to forgo batch-testing of this algorithm because it did not appear to stymie any noteworthy level of threat to the base. Despite its issues, however, this defensive concept should not be discounted entirely, as it is reasonably effective against widely dispersed or small (less than 10) numbers of enemies. As the drones are meant to support, and not supplant, current base defense

constructs, it may be acceptable for them to solely be used as an and early-warning system or interior defense against snipers while relying on counter-rocket, artillery, mortar (C-RAM)[74] systems or other defensive measures for long-range threats. Remote bases may not have these measures though, so for them, designers would need to update the passive scheme.

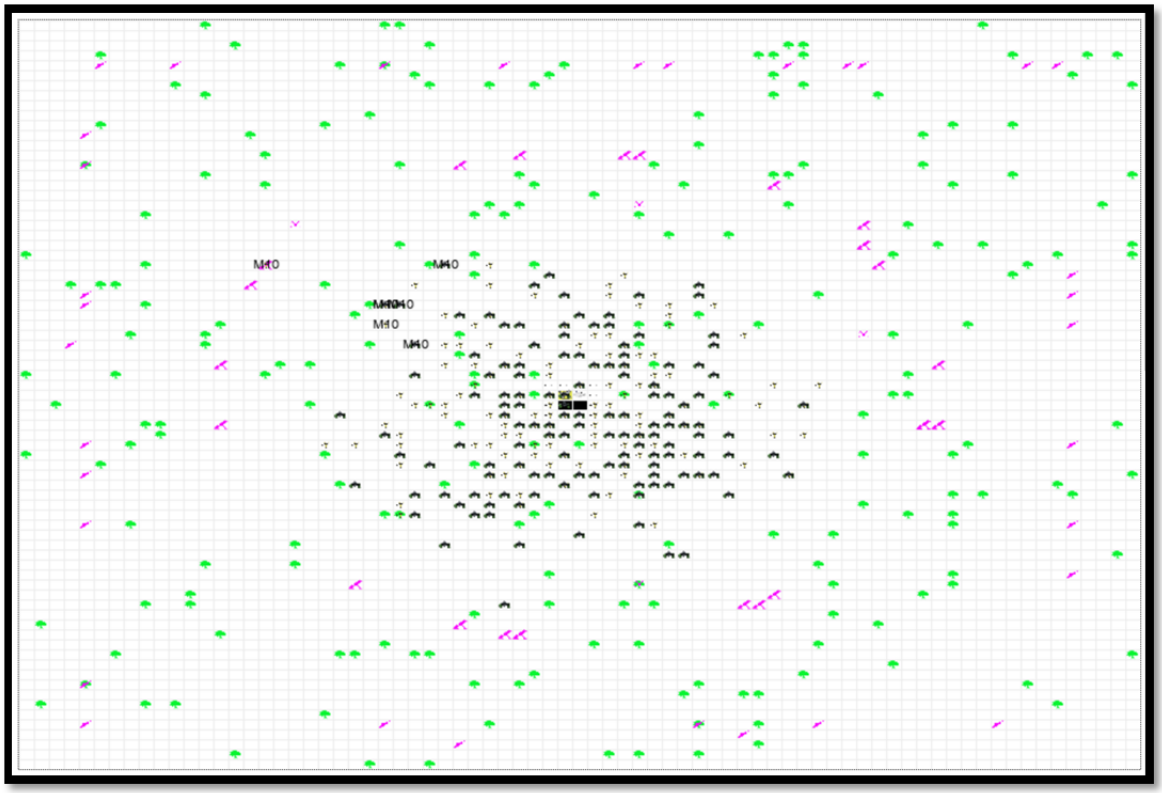
One could improve the passive algorithm by coding in limited search between grid squares in order to allow smaller swarm sizes to monitor a larger perimeter. While this allows the swarm to create a larger defensible zone, it also means that there may be a defined period of time that an enemy could exploit to move across an open area. Randomizing movement or having overlap between sectors could alleviate some ability for an enemy to simply time its movement, but this creates variability that could lead to excessive scanning of one area or larger swaths of open space as the drones attempt to scan along the perimeter. An additional option is to use the perimeter drones as a tripwire, of sorts, which trigger a reaction from the C2 element to send portions, or the entirety, of the reserve forces to the area of interest; this would leave the perimeter itself intact. The responding drones could setup in a block geometry and move as a singular unit to cover multiple grid squares during the same time before moving to the next logical location. By having a basic knowledge of an enemy's speed and exact time of first identification, the responding drones would be able to develop a basic concept of where the enemy could be by the time they arrive in the area(s) of interest.

2. Patrol Algorithm—Random

While not a logical choice for actual base defense, I analyzed the random algorithm to create a baseline for comparison against the other two patrol schemes. Swarms executing this algorithm generally failed to locate mortars because drones did not move far enough away from the base prior to the mortar shooting. Snipers, conversely, were actually caught fairly often because the swarm tended to be quite dense

[74] United States Army Acquisitions Support Center, "Counter-Rocket, Artillery, Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS)," http://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/.

(drone proximity to another) closer to the base. This provided more opportunities to locate them and since few or no bombs were used on mortars, bombers tended to be armed and nearby.



Mortars preparing to fire and drones have discovered only one mortar (#10, in northwest) at step 60.

Figure 22. Random Dispersion and Search

3. Patrol Algorithm—Grid

Under the Grid patrol algorithm, the C2's initial assignment of drones is based on mathematically dividing up the operational area (the maximum range plus the additional search area from each portion of the base) amongst the number of drones available for initial tasking (variable as to whether this includes bombers due to the user-settable parameter of having weaponized-drones airborne at the start of simulation). In testing (when combined with a "threat-based defense"), I found that while the C2's initial

dispersal design was a grid (square), the drones quickly altered their formation by moving to a more optimized circular-shaped defense. Their logic, hard-coded to correct for being beyond the search range, led to drones returning to a closer "patrol point" (the assigned position that a drone uses as a reference to start its scan from) and limiting the amount of time it spends patrolling beyond the defined threat area.

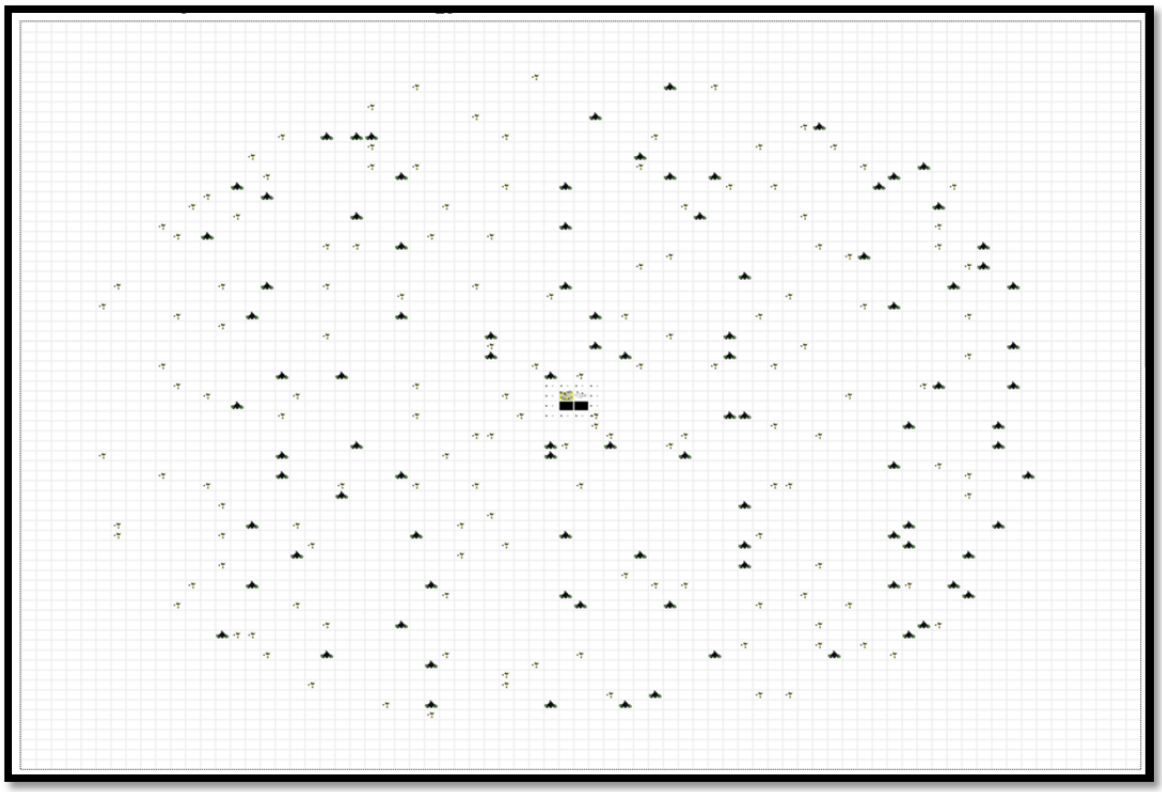


Figure 23. Circular Dispersion Due to Enemy's Threat Range

While this behavior is appropriate and desirable (in the sense that drones are aware of and correct for inefficiencies), it does indicate that designers could make improvements to dispersion in future iterations. First, using a "search range" to define a patrol space may not even be desirable. A defending commander may also desire for the drones to check a rectangular area because he may be concerned with all threats within a

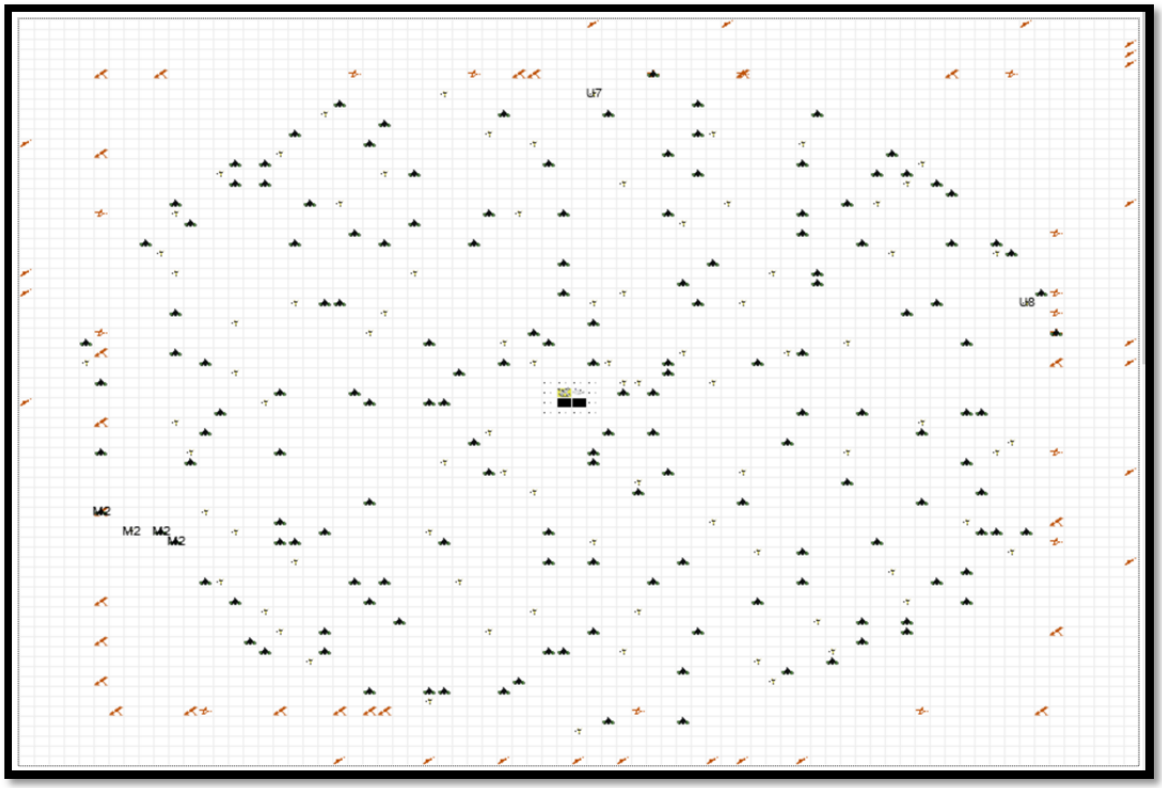
given border, or grid. As the U.S. military uses the military grid reference system[75] for many of its operations, it may be more appropriate for the drones to be responsible for anything that happens within a particular cell. Additionally, there may be other operational considerations which require this type of dispersion.

In real-world applications, and subsequent versions of this model, the option to define a non-traditional shape, or to allow the drones themselves to determine an appropriate spread based on what they encounter (mountains, cliffs, swamps, etc.) may be better alternatives. For this model, I deemed the repositioning of drones to be acceptable as it just reinforced small portions of the drone's perimeter and did not lead to excessive overlap. This algorithm appeared to be effective, and was selected for batch testing.

4. Bomber Algorithms—Dispersed and Centered

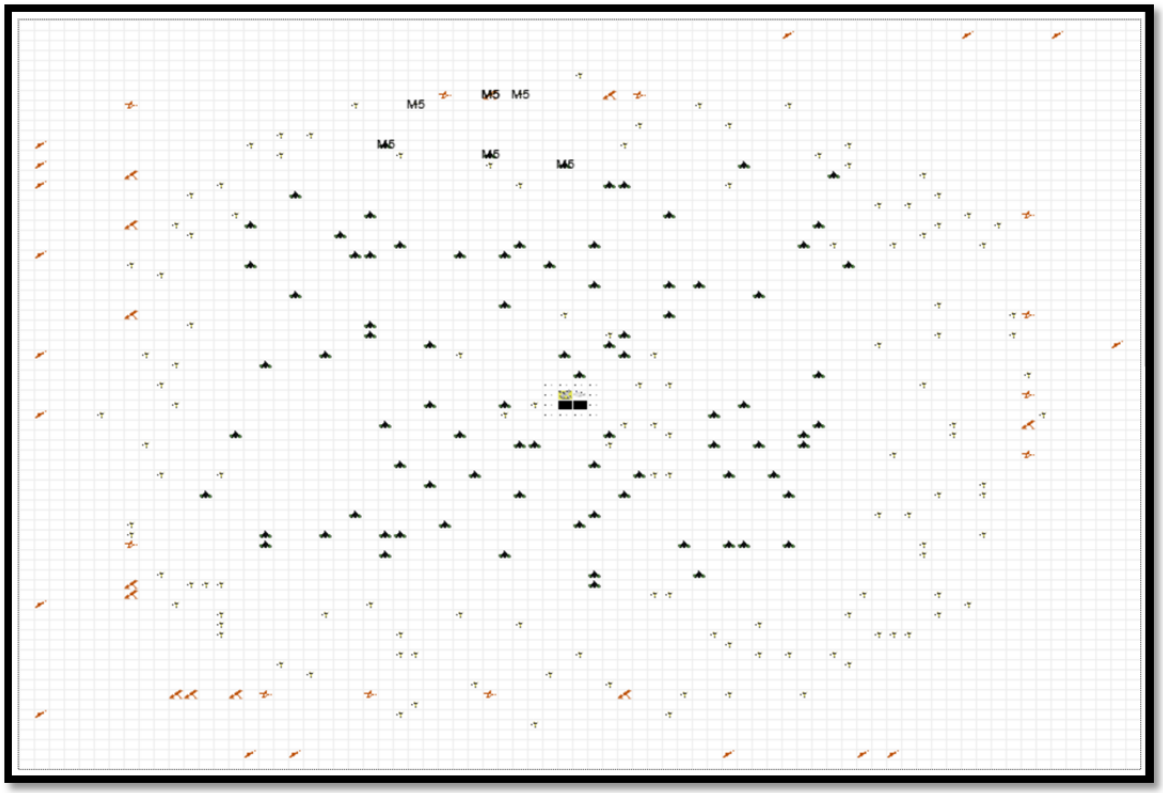
Both the dispersed and centered bomber algorithms appeared to warrant batch analysis. Swarms seemed to target enemies appropriately and with similar effectiveness under both conditions. Initial observations suggested that the dispersed algorithm may be more effective at preserving swarm integrity because bombers were able to target mortars more quickly than those patrolling just in the center. This tended to increase survivability for seekers assigned along the exterior of the patrol area. The centered algorithm appeared to showcase a swarm readily able to quickly respond to snipers that had penetrated deep into the defensive region and were close to firing positions.

[75] National Geospatial-Intelligence Agency, "Universal Grids and Grid Reference Systems, Version 2.0.0," 28 February 2014, http://earth-info.nga.mil/GandG/update/coordsys/resources/NGA.STND.0037_2.0.0_GRIDS.pdf, 3–1 – 3–10.



The swarm identifies Mortar #2 ("M2") in the southwest at step 40. Note that only the bomber that discovered the mortar and three other drones are dispatched by C2 to thwart this attacker. The C2 agent chooses the four closest entities to block the mortars shot but then recognizes that three of its blockers are bombers and does not task any further assets. This minimizes force allocation to this target and allows for more units to continue patrolling.

Figure 24. Grid Patrol with Dispersed Bombers



The swarm identifies Mortar #5 ("M5") in the north at step 40. Note here that the seeker that discovered the mortar along with the three closest assets (two seekers and a bomber) are dispatched by C2 to block the mortar from shooting. Additionally, C2 then chooses two additional, the closest, bombers which are slightly farther away due to their centrally defined patrol positions.

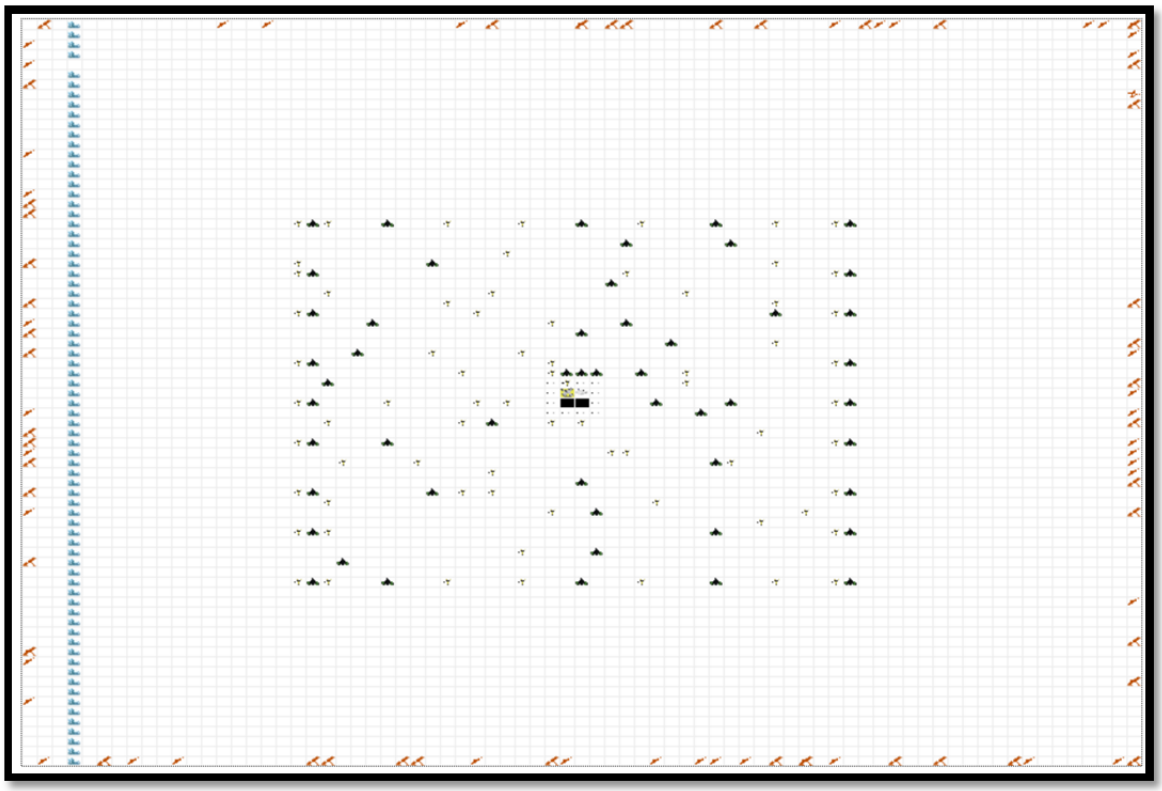
Figure 25. Grid Patrol with Centered Bombers

5. Threat-Based Defense

Most of my testing was done with a 7.5-mile grid as this allowed for the enemies to begin their approach from beyond the drone patrol area (6.8 square miles due to the mortar threat) while not exacerbating how much time it took for individual and batch iterations to complete. Because the entire area was not significantly larger than what the defenders were already patrolling, selecting non-threat-based defense did not generate a significant change in how far the drones had to patrol. Therefore, I ran all batch tests with a threat-based defense.

6. Environmental Factors

For the purposes of evaluation, I chose to only include trees in the batch processes, and not mountains. While both mountains and trees are generated using random numbers (based on the size of the model), some mountainous formations, namely ones where the range blocks all but one grid square in a quadrant, cause a substantial delay in how long it takes for the enemies to ingress (increasing the time needed to allow the model to run), and also funnel the enemies into one spot (Figure 26). This funneling, observed to some degree even with smaller mountain ranges, tended to lead to all enemies being eliminated since the defenders only had to prosecute one threat at a time instead of having multiple ones on a given side.



While an extreme example, this picture represents the funneling features of a large (randomly generated) mountain range. Enemies along the west side must all ingress through the same single pass in the northwest.

Figure 26. Mountain-Range Funneling

Future modelers improving this program may desire to either change how the mountains are constructed, change enemy behavior in routing around them, or develop drone-swarm mechanics to discern "zero-threat" areas that do not require scanning. In principle, one could incorporate this behavior into dynamic formation geometry changes where the swarm is less reliant on positional assignment from the C2 element, and instead determines its own best geometry based on a distance from the base and maintaining some separation from fellow drones. A potential danger here is, whether determined by the defending commander or by the drones themselves, in deciding that an access corridor is not traversable, defenders forfeit the opportunity to control the terrain and invite their enemies to innovate a method of ingress.

B. BATCH SIMULATION TESTING

1. Control and Test Variables

After eliminating the aforementioned algorithms, I used a batch-running process to iteratively test different scenarios in my model to help judge the significance of the remaining variables. In the batch process, as in most statistical modeling, an effective method is for modelers to hold some variables constant while varying others. In testing the Defensive Swarm model using the Mesa framework, I was able to define which of the user-defined parameters (see Chapter 3.D.2.b) would be "fixed" (constant) or "variable." I constrained the parameters' values in all simulations to be within the following fixed and variable distributions:

a. Fixed Terms

- Threat-Based Defense — On
- Steps Before Enemies Appear — 25
- Enemies — Snipers, Mortars, and UAVs
- Trees — On
- Mountains — Off

b. Independent Variables

- Patrol Algorithm — Grid, Random
- Bomber Algorithm — Dispersed, Centered
- Initial Defending UAVs — 20 to 300
- Percentage of Defending UAVs with Grenades (Bombers)—10 to 100
- Bombers Aloft — On, Off (Yes, No)
- Initial Snipers — 5 to 50
- Initial Mortars — 5 to 50
- Initial Enemy UAVs — 1 to 10

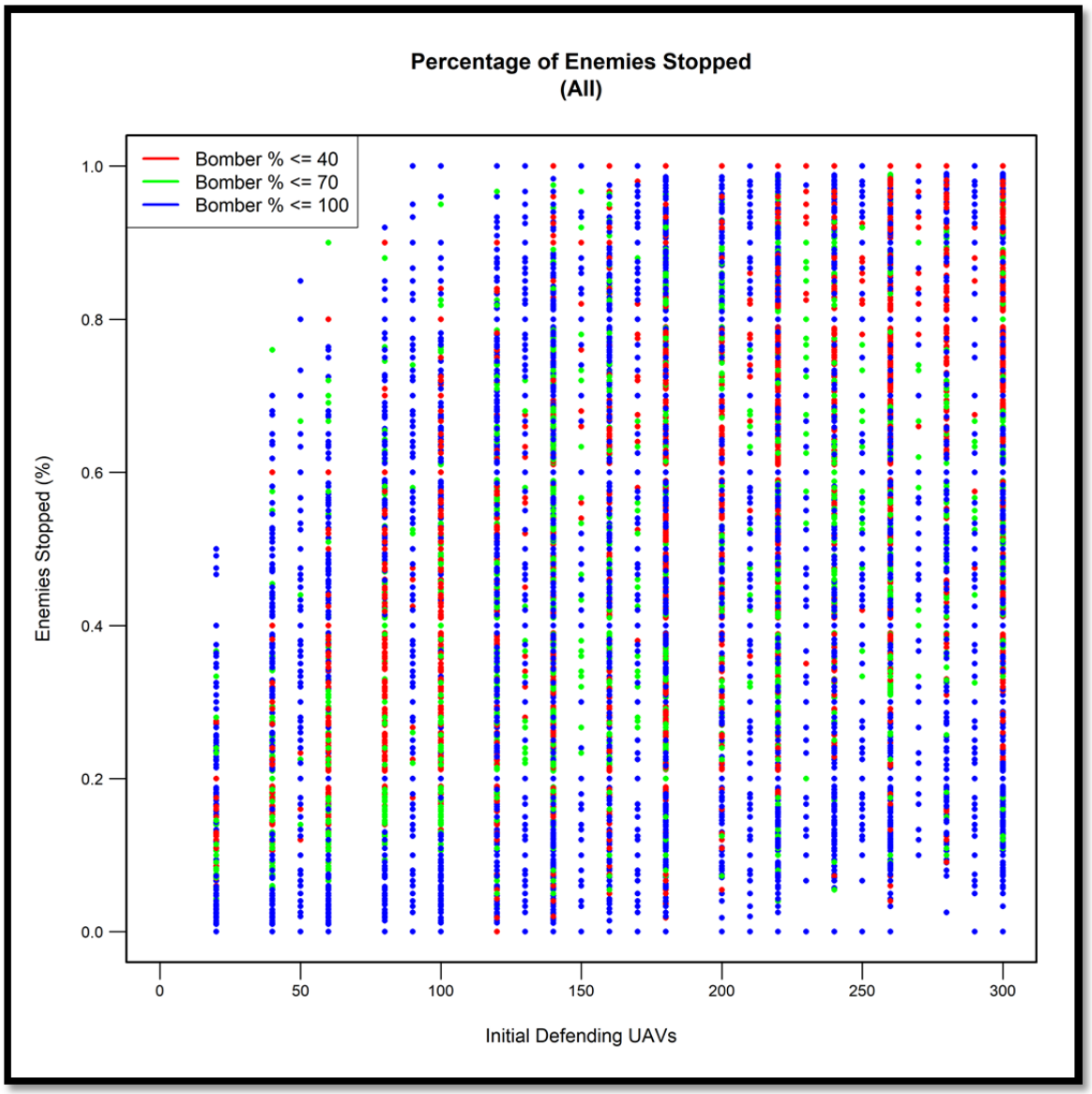
2. Results

I subjected the model to batch testing consisting of 78,580 iterations using combinations of the independent variables listed above. Overall, the drones operating under a grid-patrol algorithm were able to defend against 67.7% of attacks (Table 2). The two airborne-bomber algorithms (dispersed and centered) netted similar results with a defense-percentage average of 79.6%, but the version where the bombers had to launch from the ground (not allowed to be airborne before a swarm identifies a threat) to move towards an enemy was not as effective (44%). A swarm operating under the Random algorithm was able to stop a 45.4% of enemies, superior to the Ground algorithm, but surpassed the benchmark of blocking more than 95% of enemy attacks only once in 19,645 iterations.

Table 2. Results from Batch Simulations

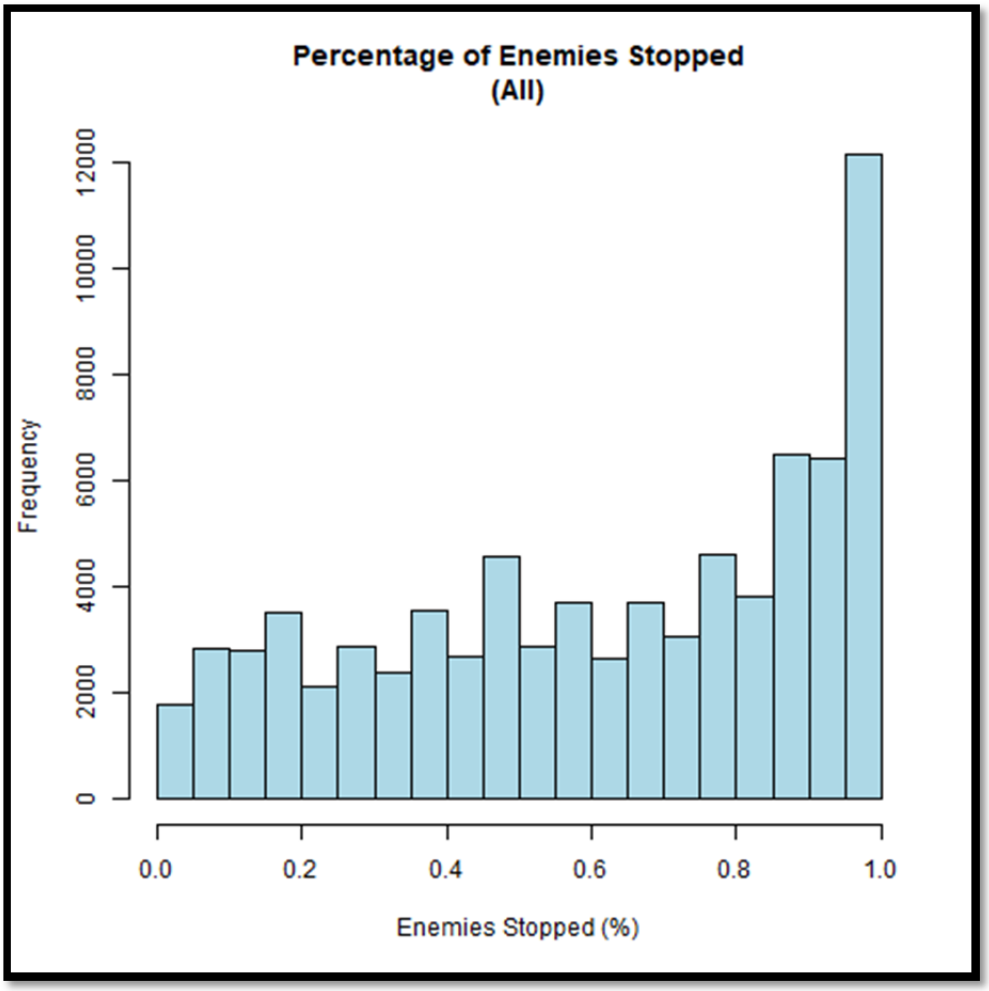
Patrol Algorithm	Bomber Algorithm	Iterations	Steps to Acquire (mean)	Steps from Find to Eliminate (mean)	Percentage of Snipers Successful	Percentage of Mortars Successful	Blocked Attack Percentage	Enemies Stopped Before Attacking Percentage	Iterations with Enemies Stopped Percentage Over 95%	Occurrence Rate (over 95%)
Grid	Centered	19645	96	17	21.7%	18.5%	60.2%	79.5%	6534	33.3%
Grid	Dispersed	19645	94	15	21.4%	18.4%	60.3%	79.7%	6826	34.7%
Grid	Ground	19645	319	24	57.5%	53.9%	22.8%	44.0%	709	3.6%
Random	Random	19645	190	10	14.2%	95.5%	41.0%	45.4%	1	0.0%
Total	-	78580	175	17	29.1%	49.6%	46.0%	62.2%	14070	17.9%

Bomber Algorithm "Ground," set by when the user variable *Bombers Airborne Before Threat* is "Off," means the bombers were not allowed to be airborne at the beginning of the simulation.



All iterations and algorithms.

Figure 27. Overall Swarm Performance



All iterations and algorithms.

Figure 28. Frequency of Percentage of Enemies Stopped before Attacking

In the scatter plot (Figure 27), the three colors represent the different bomber percentages relative to the size of the swarm denoted on the horizontal axis. With the results depicted graphically, one sees how there is no consistent correlation between an increase in swarm size and the percentage of blocked attacks. While the graphic appears to show some uncertainty overall, one does note the lack of high percentages in swarms under 100 UAVs as well as a reduction in the frequency for low-percentage results in swarms with greater than 200 UAVs.

The histogram (Figure 28) displays the frequency at which the defensive swarm was able to achieve a particular overall *enemies-stopped percentage* (listed along the horizontal axis). This success-rate chart shows a high count for 90–100% but its relative peak height is somewhat dulled by the inclusion of the results from the random search and the ground-based bomber algorithms; both of those algorithms generally had less successful results than the directed ones. This also explains the lack of clarity from the scatter plot. In fact, in order to truly analyze the effectiveness of the swarm, one must derive subsets of the data. With subsets, one can analyze the particular algorithms themselves, determine strengths, tradeoffs, and deficiencies, and develop statistical models to assist with allocating swarm sizes to a real-world problem.

a. Random Search

I utilized the batch process to test the Random Search algorithm as a point of comparison for the directed search methods. As expected, this algorithm was ineffective throughout its trials. While not a viable method for defending a base, the swarm's ability to block enemies did trend towards a normal distribution, albeit heavier-tailed on the lower half. In Figure 29, one notes not only the shape of the graph, but also the lack of results in the 95%–100% range (only one instance in all trials, 0.0051%). The random algorithm did not generate swarms able to effectively defend against mortars (4.5% stopped from attacking) and because mortars were present in all models (at least 7.7% of total enemies), the algorithm overall was unable to lead to successful defenses.

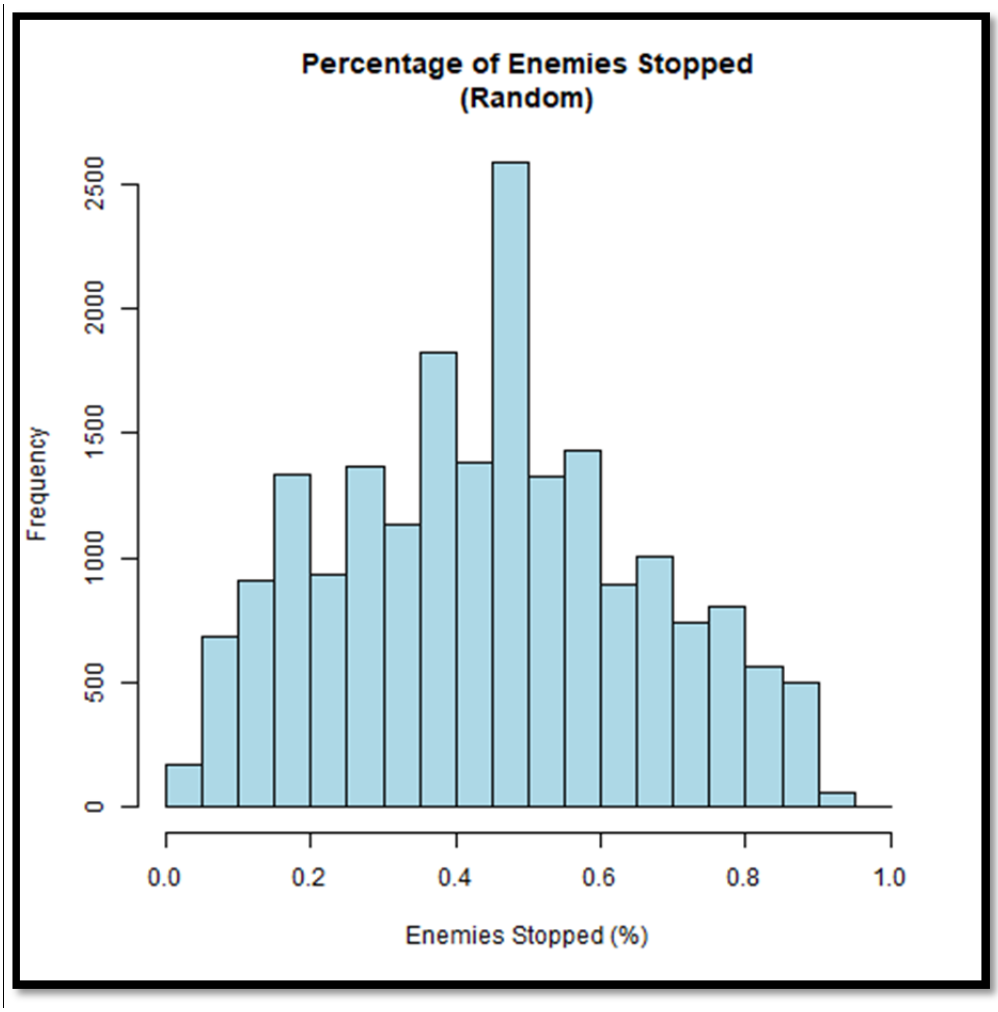


Figure 29. Random Algorithm Results Distribution

While a poor defensive algorithm, one may see the low "Steps from Find to Eliminate" value; a lower value than in many of the deliberate methods. This phenomenon occurs because the swarm density in the random algorithm tends to stay higher than the grid patrol algorithm as many drones fail to maneuver a substantial distance away from the base. Bombers, then, whether smaller or larger percentages of the total swarm, are more likely to be near an enemy since the enemy is often discovered very late in its ingress phase (close to the base). As observed in the single-run tests, snipers were then caught, and eliminated, at a relatively high rate because of the likelihood for multiple drones to observe them and be available for immediate targeting.

b. Grid Patrol with Centered, Dispersed, and Ground Bomber Algorithms

The main objective of my batch analysis was to determine whether the centered or dispersed bomber algorithm was the most effective. Through 39,290 iterations, the drones operating with airborne bombers achieved an average stop-enemy percentage of 79.6% and achieved higher than 95% stops in a third of all trials. When user options relegated bombers to launch from the ground after enemy contact, the swarm still generally performed well in acquiring and stopping mortars, but due to the increased time for the bombers to travel to and eliminate an enemy far from the base, mortars tended to kill the exterior seekers that had found and were blocking its firing path. This action results in a successful block for the defenders, but creates two second-order problems. First, since there are fewer drones in the swarm (no reinforcements), it is less-likely that a sniper will be discovered. Second, since the swarm does not dynamically resize after a loss, if there was a second wave of enemies (not modeled), there would be fewer drones patrolling at the distance from which a mortar could shoot.

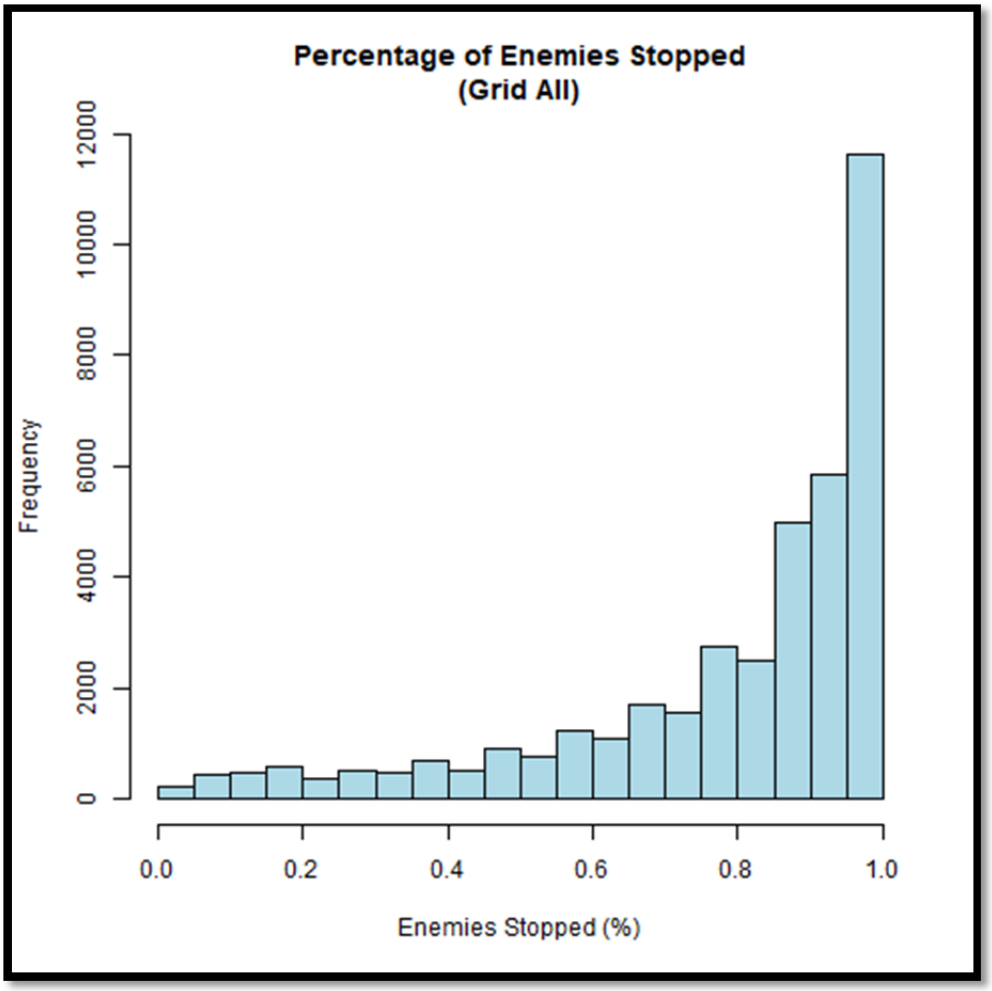


Figure 30. Percentage of Enemies Stopped under Grid-Patrol Algorithms

The Centered and Dispersed bomber methods achieved quite similar results. Their *Steps to Acquire* metrics should be exact, as there is no difference in the inherent search pattern, just where the bombers are in the formation. However, as discussed later, mortars have a higher likelihood of killing seekers in the centered bomber formations, which leads to an overall smaller swarm and could cause this deviation. The centrally-confined bombers are, however, likely the reason for the "Steps from Find to Eliminate" being slightly higher for that type of swarm. Bombers must travel farther to target enemies discovered early in the simulation and, logically, take longer to get to an enemy. Conversely, there should be ample bombers available to quickly target a sniper that has penetrated the defensive perimeter.

With the dispersed algorithm, if a bomber along the periphery of the formation uses its ammunition early in the simulation, it will RTB and rearm. The snipers move six-times slower than drones, so often times, a bomber can attack a mortar, RTB, and re-launch to arrive back in its patrol zone before a sniper can move through it completely (other drones also continue to patrol the bomber's area during its absence due to designed overlap). While the centered-bomber algorithm will have more bombers to target a close-in sniper, only one grenade is needed to kill the sniper, so the dispersed formation does not suffer a major loss in response time (if any). A lower response time for eliminating a target, is therefore likely an attribute of the dispersed swarm. One should note that the size of the defensive area could drastically affect the difference between response times for dispersed and centrally-located bombers, especially when the bomber fleet or overall swarm size is low in quantity.

The values presented in Table 2, while comprehensive, are not fully representative of the effectiveness of swarms of a given size. To further refine the evaluation and to determine which combinations of swarm density and composition achieves the highest success rate, one must continue to split the statistics into more specific categories. This type of analysis is instructive in developing recommended courses of action for base commanders.

In order to determine the correlation of an algorithm's operation to effectiveness, I ran 36,000 iterations of the model using a constant set of parameters (24,000 of strictly grid-patrol algorithm models). While all iterations assist in overall modeling, in order to ascertain any relationship between various swarm sizes or algorithms, one must use a consistent set of variables to subject each type of swarm to the exact same testing. In Tables 3, 4, and 5, I show the differences in results between swarms of the two airborne-bomber algorithms (blue, orange) and the ground algorithm (green).

Previous testing indicated that swarms smaller than 140 UAVs rarely stopped 50% of the enemies and virtually never achieved a 95%-success rate. Therefore, for this test, the smallest swarm consisted of 140 UAVs. While not likely to be successful in defense, the swarm's performance at that size could lead to insight or provide a point of comparison for larger swarms. Bomber percentages ranged from 10% to 100% by

increments of 30%. Hence, in the tables, one sees the swarms divided by the number of UAVs, and then by bomber percentage.

Table 3. Results from Simulations: Grid Patrol with Centered Bombers

Swarm Size	Bomber Percentage	Iterations	Steps to Acquire (mean)	Steps from Find to Eliminate (mean)	Percentage of Snipers Successful	Percentage of Mortars Successful	Blocked Attack Percentage	Enemies Stopped Before Attacking Percentage	Iterations with Enemies Stopped Percentage Over 95%	Occurrence Rate (over 95%)
140	10	450	167	64	52%	33%	27%	58%	8	2%
140	40	450	70	9	23%	24%	46%	75%	3	1%
140	70	450	67	6	20%	26%	50%	76%	22	5%
140	100	450	63	8	17%	18%	54%	81%	28	6%
180	10	450	115	59	40%	20%	38%	71%	30	7%
180	40	450	50	9	13%	11%	66%	88%	65	14%
180	70	450	49	5	12%	11%	67%	88%	83	18%
180	100	450	45	8	9%	7%	73%	92%	151	34%
220	10	450	80	50	26%	16%	53%	79%	77	17%
220	40	450	42	8	10%	8%	72%	90%	105	23%
220	70	450	43	5	9%	8%	73%	91%	128	28%
220	100	450	39	8	6%	4%	80%	94%	252	56%
260	10	450	55	50	18%	8%	64%	87%	171	38%
260	40	450	31	8	5%	3%	83%	96%	292	65%
260	70	450	33	5	6%	4%	84%	95%	262	58%
260	100	450	30	9	5%	1%	83%	97%	357	79%
300	10	450	46	44	11%	7%	75%	91%	206	46%
300	40	450	28	8	2%	1%	93%	98%	421	94%
300	70	450	28	5	3%	3%	91%	97%	350	78%
300	100	450	26	9	2%	1%	92%	98%	415	92%

Table 4. Results from Simulations: Grid Patrol with Dispersed Bombers

Swarm Size	Bomber Percentage	Iterations	Steps to Acquire (mean)	Steps from Find to Eliminate (mean)	Percentage of Snipers Successful	Percentage of Mortars Successful	Blocked Attack Percentage	Enemies Stopped Before Attacking Percentage	Iterations with Enemies Stopped Percentage Over 95%	Occurrence Rate (over 95%)
140	10	450	165	61	52%	35%	26%	56%	4	1%
140	40	450	71	8	25%	24%	45%	74%	8	2%
140	70	450	66	5	19%	22%	52%	78%	18	4%
140	100	450	62	8	16%	18%	54%	82%	26	6%
180	10	450	105	51	35%	23%	40%	71%	29	6%
180	40	450	51	7	14%	12%	63%	86%	67	15%
180	70	450	48	5	11%	9%	70%	90%	105	23%
180	100	450	46	8	9%	7%	73%	92%	144	32%
220	10	450	77	43	23%	17%	52%	79%	64	14%
220	40	450	43	6	9%	7%	75%	92%	158	35%
220	70	450	41	4	8%	6%	78%	93%	190	42%
220	100	450	40	8	7%	4%	79%	94%	226	50%
260	10	450	54	43	17%	9%	62%	87%	121	27%
260	40	450	31	5	5%	2%	84%	96%	343	76%
260	70	450	31	4	6%	2%	83%	96%	325	72%
260	100	450	30	8	5%	1%	84%	97%	361	80%
300	10	450	46	37	10%	7%	74%	91%	194	43%
300	40	450	28	5	3%	1%	91%	98%	404	90%
300	70	450	27	4	3%	1%	92%	98%	412	92%
300	100	450	26	9	2%	1%	92%	98%	420	93%

Table 5. Results from Simulations: Grid Patrol with Ground-Based Bombers

Swarm Size	Bomber Percentage	Iterations	Steps to Acquire (mean)	Steps from Find to Eliminate (mean)	Percentage of Snipers Successful	Percentage of Mortars Successful	Blocked Attack Percentage	Enemies Stopped Before Attacking Percentage	Iterations with Enemies Stopped Percentage Over 95%	Occurrence Rate (over 95%)
140	10	450	184	68	57%	34%	24%	55%	4	1%
140	40	450	127	18	50%	44%	22%	52%	0	0%
140	70	450	233	16	73%	71%	10%	28%	0	0%
140	100	450	733	15	90%	93%	3%	8%	0	0%
180	10	450	123	56	39%	27%	36%	67%	19	4%
180	40	450	95	17	38%	34%	30%	63%	1	0%
180	70	450	200	17	67%	62%	12%	35%	0	0%
180	100	450	539	16	86%	89%	4%	13%	0	0%
220	10	450	89	55	29%	16%	46%	77%	45	10%
220	40	450	76	17	29%	23%	39%	73%	6	1%
220	70	450	155	17	58%	55%	16%	43%	0	0%
220	100	450	457	16	82%	88%	5%	14%	0	0%
260	10	450	70	50	21%	12%	56%	84%	94	21%
260	40	450	63	16	21%	17%	50%	80%	15	3%
260	70	450	136	16	51%	54%	20%	47%	0	0%
260	100	450	398	17	84%	82%	5%	17%	0	0%
300	10	450	52	46	12%	8%	68%	89%	150	33%
300	40	450	53	17	16%	11%	58%	85%	49	11%
300	70	450	116	17	46%	44%	24%	54%	0	0%
300	100	450	357	17	81%	80%	6%	20%	0	0%

In Tables 3 and 4, one recognizes the nearly congruent rise of how many enemies are stopped relative to the swarm size regardless of the bomber algorithm. Swarms with 220 UAVs and at least 40% bombers are able to deter 90% or more of the attackers. Minor variations between percentiles are possibly due to the random placement of enemies on the map, or the probabilistic nature of the agent interactions during the drones' search and engagement profiles. This potential randomness is evident in the 100% bomber-swarms, where there is no difference between the two airborne algorithms, yet they still have minor deviations in success percentages. What is striking, however, are a few statistics that have larger differences between the two algorithms.

First, there appears to be a distinct advantage, at 10% bombers, for the dispersed swarms in their ability to defeat enemies quicker than the centered ones. If one discounts the ineffective 140-sized UAV swarms, a trend emerges where the dispersed-bomber swarms attack their targets 7–8 steps (105–120 seconds) faster than an equivalently sized centered-bomber swarm. Note, however, that with larger bomber percentages, this advantage disappears.

Another finding is that all dispersed swarms with 70% bombers, and most with 40% bombers, outperform their centered counterparts by values ranging from 5%–14% with regard to how many times the swarms stop greater than 95% of the attackers. Again, the overall effectiveness between the two algorithms is quite similar, indicating that across the range of simulations, they have similar performance characteristics. A curious outlier, is that in trials with the centered-bomber swarm with 260 UAVs and 10% bombers, it outperforms the dispersed variant by 11%. This could be an issue with the dispersed algorithm in that at this particular size, with so few bombers, that the bombers are simply patrolling too far away from base to quickly respond to snipers that have made it fairly close to the base before the drones discover them. More testing is necessary to see if this trend continues, or if this is an abnormality caused by random variation in the simulation (during either the centered or dispersed trials).

Overall, the dispersed swarms' ability to achieve higher counts of stopping more than 95% of enemies is potentially attributable to the previously mentioned concept that a

centered-bomber swarm suffers from losing exterior seekers during a successful blocking of a mortar. Unlike the dispersed swarm, which features drones returning to their patrol position after a mortar is bombed, the centered bombers lose some effectiveness along the perimeter once sub-swarms of seekers assigned to block the mortar tubes die during defensive operations. This problem is potentially more pronounced with middling numbers of bombers because swarms with only 10% bombers are somewhat equally likely to be unable to maneuver enough bombers to defeat larger numbers of mortars along the perimeter. The centered-bomber swarms stop the attack with seekers, while the dispersed ones appear to be able to bomb the mortars more quickly. This phenomenon also likely explains why the *Steps to Acquire* metric is so much higher (nearly double) in 10%-bomber swarms than swarms of the same size but with higher bomber percentages.

Thus, the dispersed-bombers obtain a slight advantage when bomber counts are in the 40%–70% range by having a higher likelihood of being able to quickly maneuver a team of bombers to attack a mortar before shooting. While more bombers will need to RTB to rearm, more seekers will remain alive and continuing to assist with the search. As the number of bombers increases beyond 70%, so does the distance that a bomber may be from a base in its assigned patrol position. Therefore, the two types of algorithms should achieve similar results at higher-bomber percentages and results should be equivalent once the entire formation consists of bombers.

The results from the ground-based bomber simulations (Table 5) were not overly promising, but that is largely expected. I constructed this algorithm in order to study the potential usefulness of a swarm in situations where bombers could not be a part of the persistent, airborne-swarm. In Table 5, one sees an inverse relation between the percentage of bombers and the effectiveness of the swarm. This happens because as that percentage increases, more of the formation is confined to the runway awaiting orders. Therefore, the most applicable numbers from this table are from the 10%-bomber swarms. Although they were not as effective as the airborne variants, these data still demonstrate that these swarms could potentially be of use even with limited rules of operation.

3. Statistical Models

I aggregated the results of the simulations and used them as an input into a statistical modeling script that I wrote using R, "a free software environment for statistical computing and graphics."[76] I formulated generalized-linear models to examine how the independent variables, or corresponding interactions amongst them, aligned with the successfulness of the defensive swarm. In these models, the dependent variable was the percentage of enemies the drones blocked from attacking, relative to the total number of possible attacks.

I developed and tested over 30 different statistical models, but am reporting only the final four that best portray both swarm effectiveness and also the importance of individual variables. These models had statistically significant coefficients with substantive effects, and also had the lowest Akaike Information Criterion (AIC) scores, which indicate relative superiority to the other models given a particular dataset.[77] To compare swarm effectiveness across the range of conditions, I developed two separate types of models.

The first type of model compared swarms based on using all descriptor variables (initial drones, bomber percentage, initial mortars, etc.) but also applied relationship terms of *Seeker Ratio* and *Bomber Ratio*. *Seeker Ratio* is the number of seekers compared to the total number of enemies in the model. *Bomber Ratio* is similar, but the number of Enemy UAVs is not considered because, by design, a bomber does not target an Enemy UAV. The *bomber ratio,* therefore, is strictly the relationship of bombers to the enemies which maneuver on the ground.

---

[76] The R Foundation, "The R Project for Statistical Computing," https://www.r-project.org/about.html.

[77] Mike Christie, Andrew Cliffe, Philip Dawid, and Stephen S. Senn, eds, *Simplicity, Complexity and Modelling* (New York: John Wiley & Sons, Incorporated, 2011), ProQuest Ebook Central, 21–22.

The second type of model removes the ratio terms and instead attempts to gauge the importance of the interaction between the number, and type, of offensive and defensive units. This interactive modeling creates additional terms that are only applicable to the model in which the interaction occurs. As a result, in cases where either I stop using the first type of model, or use a different set of interactions, a blank space for that term appears in the statistical model table (Table 6).

a. Statistical Model Description

The four models presented here fall within the previously mentioned two categories of models. Models 1 and 2 use the ratio terms, while Models 3 and 4 utilize the interaction between offensive and defensive agents. Model 1 (m1) analyzes the basic combination of initial drones, mortars, snipers, Enemy UAVs, the percentage of bombers in the formation, as well as seeker and bomber ratios. Model 2 (m2) has the same variables but introduces an interactive term, *(Defending UAVs :: Bomber %)* which I refer to as the "Drone-Bomber" term; the value of this term is dependent on both values simultaneously, their interactive effect. In Model 3 (m3), I remove the ratio terms and the "Drone-Bomber" term and instead allow the interaction between defenders and enemies to account for that information. Model 3's interaction, then, is between each defensive and offensive unit individually. Finally, Model 4 (m4) uses the same interactive methodology as Model 3, but I add the "Drone-Bomber" term back in, which then creates an additional set of interactions, those between the "Drone-Bomber" term and each of the enemy units.

Table 6. Defensive Swarm Statistical Models

Defensive Swarm Models (Grid All)

	Dependent variable:			
	Percentage of Enemies Stopped Before Attacking			
	m1	m2	m3	m4
	(1)	(2)	(3)	(4)
Initial Defending UAVs	0.017***	0.011***	0.023***	0.023***
	(0.0004)	(0.001)	(0.001)	(0.001)
Bomber %	0.016***	0.006***	0.002	0.004
	(0.001)	(0.001)	(0.001)	(0.003)
Initial Mortars	-0.026***	-0.025***	-0.030***	-0.011**
	(0.001)	(0.001)	(0.003)	(0.005)
Initial Snipers	-0.0002	0.001	-0.006**	-0.010**
	(0.001)	(0.001)	(0.003)	(0.005)
Initial Enemy UAVs	-0.004	0.0001	-0.0002	0.003
	(0.004)	(0.004)	(0.014)	(0.020)
Seeker Ratio	0.130***	0.238***		
	(0.019)	(0.023)		
Bomber Ratio	0.046***	-0.008		
	(0.013)	(0.012)		
(Defending UAVs :: Bomber %)		0.0001***		-0.00000
		(0.00001)		(0.00002)
(Defending UAVs :: Mortars)			-0.0001***	-0.0002***
			(0.00002)	(0.00003)
(Defending UAVs :: Snipers)			-0.00005***	-0.00002
			(0.00002)	(0.00003)
(Defending UAVs :: Enemy UAVs)			-0.0001*	-0.0001
			(0.0001)	(0.0001)
(Bomber % :: Mortars)			0.0003***	-0.0001
			(0.00003)	(0.0001)
(Bomber % :: Snipers)			0.0001***	0.0002***
			(0.00003)	(0.0001)
(Bomber % :: UAVs)			0.0001	0.0001
			(0.0001)	(0.0003)
(Def. UAVs and Bomber % :: Mortars)				0.00000***
				(0.00000)
(Def. UAVs and Bomber % :: Snipers)				-0.00000
				(0.00000)
(Def. UAVs and Bomber % :: Enemy UAVs)				0.00000
				(0.00000)
Constant	-1.846***	-1.400***	-1.434***	-1.519***
	(0.084)	(0.092)	(0.126)	(0.188)
Observations	39,290	39,290	39,290	39,290
Log Likelihood	-7,834.892	-7,754.810	-7,720.826	-7,723.443
Akaike Inf. Crit.	15,685.780	15,527.620	15,465.650	15,478.890
Note:				*p<0.1; **p<0.05; ***p<0.01

The results of the models show a high level of statistical significance ($p < 0.01$) for many variables in how they affect the percentage of blocked attacks. The notable exceptions are *Bomber Percentage* (m3, m4), *Initial Snipers* (m1, m2), *Initial Enemy UAVs* (all), *Bomber Ratio* (m2), and some of the interactive terms. While these terms are still part of the model, they are not statistically significant at even the $p < 0.1$ level.

The statistical insignificance of the *Bomber Percentage* term in the last two models, and for *Bomber Ratio* in Model 2, is likely because the variable's effect is accounted for by the interactive terms. In fact the only two variables which maintain a statistical significance (at least $p < .05$) throughout all models are *Initial Defending UAVs* and *Initial Mortars* (though *Seeker Ratio* is significant in each of the two models it appears in). The interaction between these two terms (m3, m4) is also deemed to be of high significance ($p < 0.01$).

The absence of *Initial Snipers* from the list of statistically significant terms, in Models 1 and 2, is an unexpected finding. Still, there are possible explanations for this evident within the table itself. In those models, the two ratio terms include the number of snipers and it may be that mortars, significant on their own, are simply more dangerous to the base's safety because of their range and the fact that they may destroy defending UAVs during the contest.

The fact that the *Enemy UAV* term and any interactions involving it do not factor heavily into the model's importance is due to the somewhat limited effect that Enemy UAVs themselves have in the scenario. While Enemy UAVs do not target the base or achieve successful attacks themselves, they do serve as another target for the drones to track. Any drone that is not in its patrol position presents an opportunity for increased-ingress success for a sniper or mortar unit. Therefore, while the term is generally insignificant (one interactive term in m3 is significant at the $p < 0.1$ level) to these statistical models, further testing with higher volumes of UAVs could change the importance of the term, even without adding any more capability to the units within the Defensive Swarm agent-based model.

Otherwise, one sees a significant, positive correlation between the percentage of enemies stopped before attacking and an increase in *Initial Defending UAVs or Bomber Percentage* (including interactive) terms. Correspondingly, either the *Initial Mortars* or *Initial Sniper* term or a form interaction involving them have statistically significant, negative coefficient relationships with the likelihood of the swarm stopping attacks (more enemies trend towards more successful attacks and a poorer defense).

Finally, one should observe the AIC scores for the various models. Models 1 and 2 are the weakest. Models 3 and 4 score nearly identically, but the AIC method penalizes models for additional terms, which may account for the difference. Model 3 ultimately achieved the lowest (superior) score. However, both models, due to their statistically significant coefficients, merit further analysis.

b. Analysis of Statistical Models

To conduct a supplementary evaluation of Models 3 and 4, it is useful for one to analyze statistically significant variables using estimates of substantive effect sizes. I created visual regression plots that display the outcomes of the models with regard to the two airborne-bomber algorithms. The graphs, in Figures 31 and 32, depict the results of the parameters using the coefficients from Table 6. Along the vertical axis, one sees the resultant percentage of enemies the drones should stop before the adversaries could attack the base. The horizontal axis shows the number of Defending UAVs. Rather than a single line or scatter plot, I use four individually-colored lines to show the results of various bomber percentage levels relative to the total number of Defending UAVs. The red, green, blue, and purple lines represent the model's results for a given UAV value paired with the distinct values listed in the legend for the percentage of bombers in the formation.

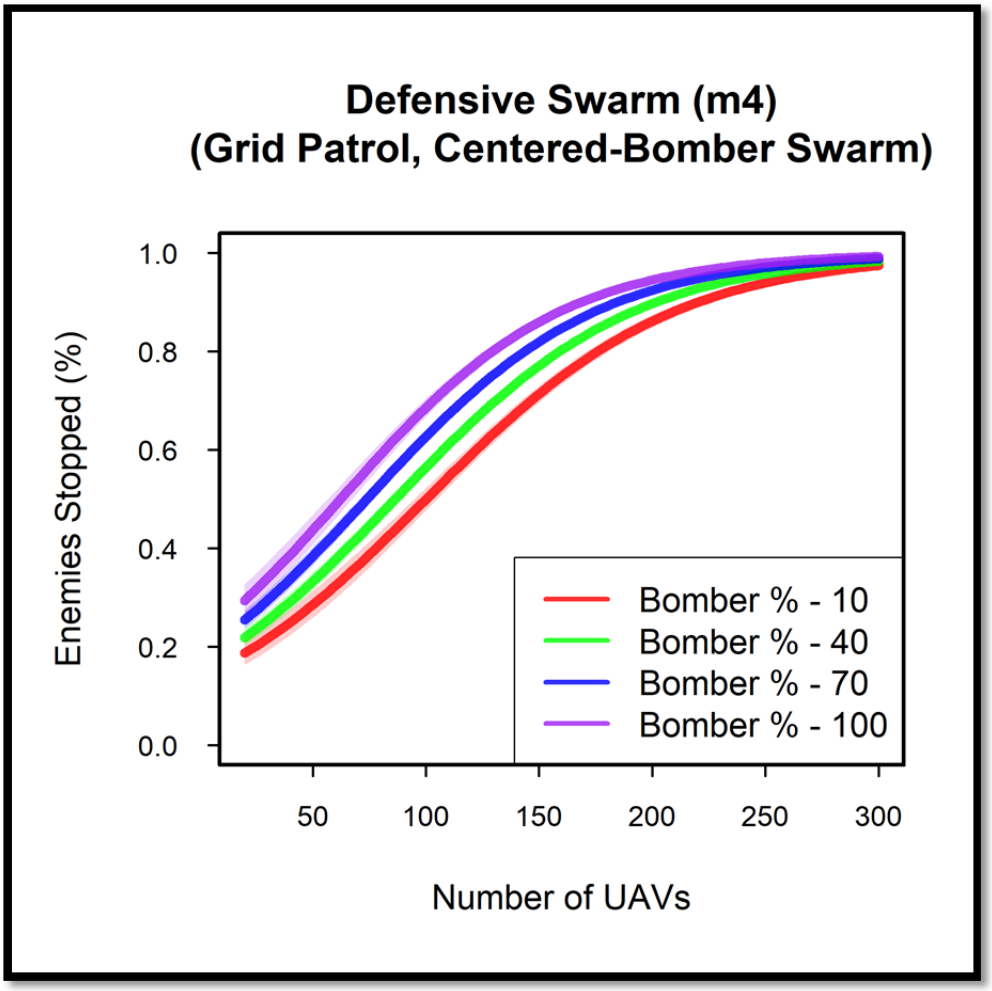


Figure 31. Statistical Model of Grid Patrol with Centered Bombers

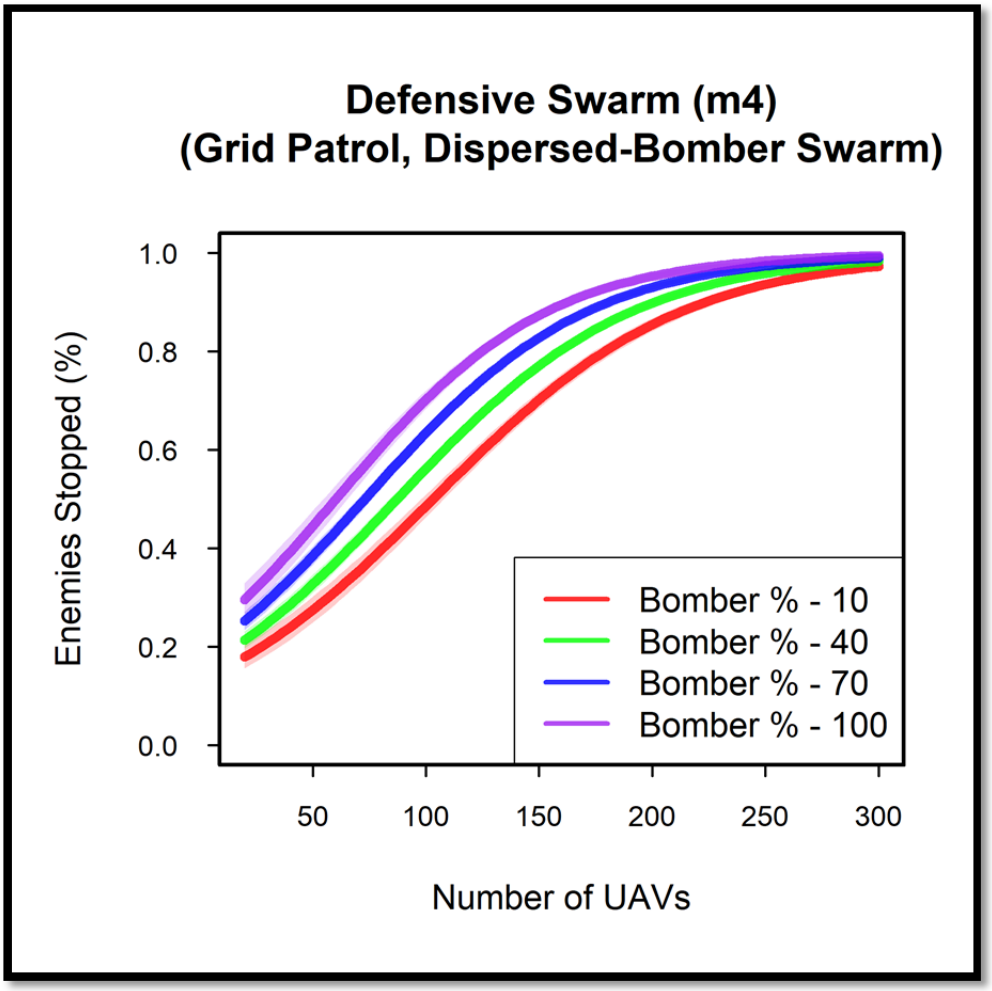


Figure 32. Statistical Model of Grid Patrol with Dispersed Bombers

The overall shape and slope of both graphs show that as the number of defending UAVs increase, so does the percentage of enemies the drones stop. By using the bomber percentage to differentiate the results, one can discern levels of effectiveness between various compositions of swarms. While slight, one should also visually distinguish the shaded area (a 95% confidence band) around each line. This shaded area is particularly noticeable at the left edge (*Number of UAVs* = 20) of the red and purple lines and illustrates an area of uncertainty; an area in which the model is less exact and has a broader range in which the results could exist. Here, the relatively small, and with minimally overlapping, bands indicate that the statistical model is generally unambiguous in its ability to determine a likely outcome for a given set of parameters. Additionally, it

appears to be more exact in its determinations at UAV values greater than 100 (the confidence band shrinks).

Under closer scrutiny, one observes when there are fewer UAVs, instances of swarms with larger bomber numbers are able to perform slightly better. In smaller swarms, a greater bomber percentage can increase effectiveness by roughly 10%, but in larger swarms, it becomes less important to the overall result. As bombers can perform any action that a seeker does, it is sound to expect a sufficiently-sized swarm to be able to overcome having a small amount of seekers, since they mainly serve as a frontline defense against Enemy UAVs and as a blocking force overhead mortars that have not been attacked by bombers. Consequently, the swarms with the smallest number of Defending UAVs and bomber-percentage subsets suffer due to low density (increased coverage requirements per drone) and generally tally significantly lower defense percentages.

When the bomber-force sizes are low (red lines), it becomes increasingly more important to have more seekers until the overall effectiveness begins to converge as swarm sizes approach 200 UAVs. There is a two-fold explanation for this. First, seekers have the ability to thwart a mortar attack without any support from bombers (via the hovering over muzzle technique). The C2 agent prioritizes sending bombers to target snipers, however, if the seekers find mortars prior to snipers, which is invariably the case due to the mortar's faster speed, the C2 agent will send bombers to attack them as no higher-priority target exists.[78] By eliminating the mortars with bombers, the overall health of the swarm is improved because there is no need to sacrifice any sub-swarm of seekers assigned to block mortars. Therefore, the second explanation is that with an increase in seekers, it is more likely that mortars will be discovered earlier, allowing for bombers to attack them before the mortars fire (aided by the C2's prioritization function and subsequent reallocation of bomber assets). If successful, the swarm benefits from preserving more seekers to continue to search for other enemies.

[78] The logic is that the seekers hovering above a mortar will stop the shell, while the seekers tracking the sniper cannot stop him from firing.

Otherwise, once a swarm is at or greater than 200 drones, the model suggests that they will score consistently in the 80–95% range, regardless of the number of bombers present in the formation. These data support the logic from the preceding paragraph in that at a certain size, the swarm simply patrols the area faster and more often. At 200 drones, with bombers accounting for as little as 10% of the total swarm, the swarm can still obtain a defense percentage of 80%.

When viewing the interactions from Model 3, using similar chart construction, but different variables, one better sees the impact of the different coefficients to the interaction terms listed in Table 6. The first graph of Figure 33 shows the interaction between the overall number of defending UAVs and the number of mortars. In it, one observes a similar shape to the previously displayed graphics. This is expected given the consistent statistical significance of the mortar term in all models and its seeming importance to the overall model. The second graph demonstrates the interaction of the bomber percentage term coupled with the number of mortars present in a model. This graph shows that a larger mortar force has a substantive effect on the overall result and it is most significant at lower bomber percentages.

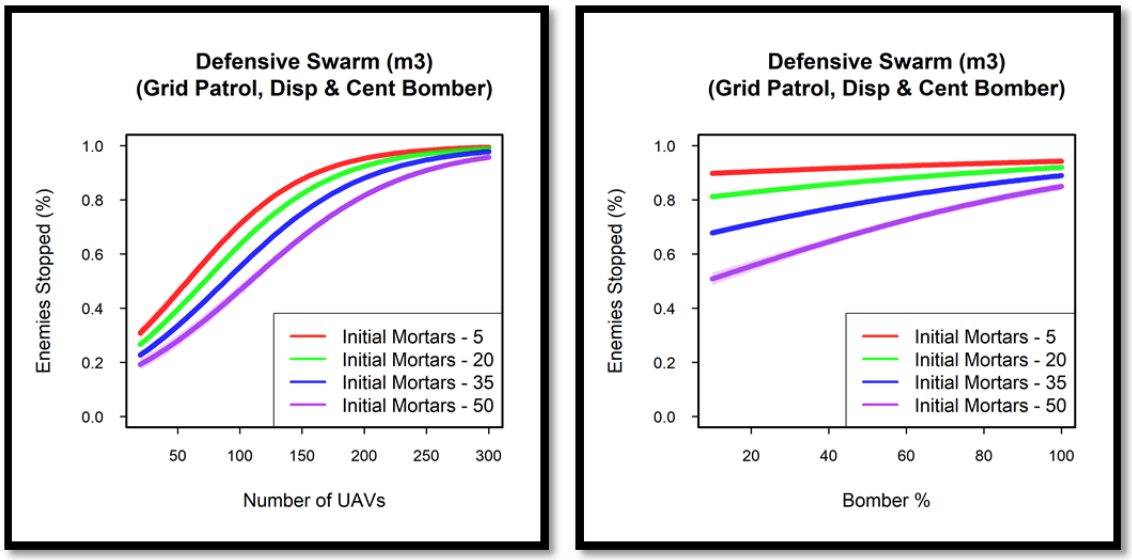


Figure 33. Statistical Model of the Defending Swarm Paired with the Number of Mortars

When analyzing the same independent variables' interaction with snipers (Figure 34), once again one sees the same shape in the first graph, but this time not the individual lines. When snipers are paired with the bomber percentage term, a similar almost coincident line appears. These results indicate that though the sniper has an important effect on the overall percentage, that the unit's effect is more consistent across the range of sniper force counts, as well as against various bomber fleets.

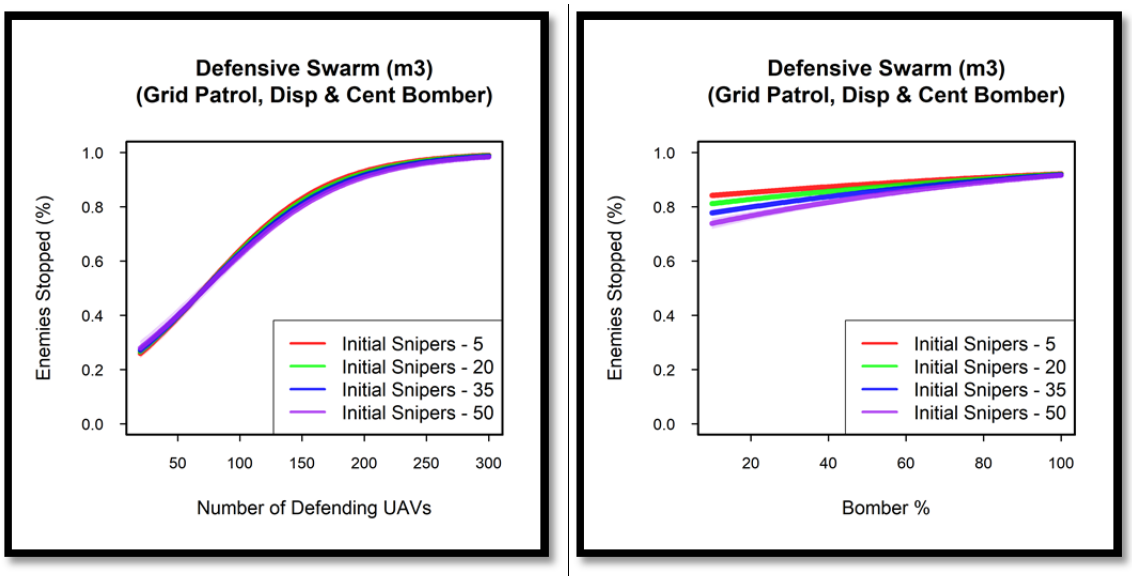


Figure 34. Statistical Model of the Defending Swarm Paired with the Number of Snipers

Invariably, a higher swarm density after the mortars are killed or have fired is tantamount to stopping the snipers. Drone formations must be dense enough to patrol the area and get enough chances to find the furtive snipers. During this search period, the swarm benefits from the sniper's long travel route towards the base and also the ease in which they can eliminate him due to his lack of armor. With the bombers only needing to successfully conduct one grenade strike (at probability of kill of 90%), if the swarm has more than a one-to-one ratio of grenades-available to snipers-remaining then it is very likely that the swarm can successfully finish defending in the scenario, provided it can locate the remaining threats.

4. Receiver Operating Characteristic

A final way that I used to evaluate the defenders was utilizing a receiver operating characteristic (ROC) graph (Figure 35). A ROC graph depicts where the model correctly guessed the result (True Positive) compared to when it thought it should be positive, but then was wrong (False Positive). To set the binary nature of whether the prediction was correct, I set a threshold value of 95% success in stopping enemies before attacking, and ran separate logit regressions on this binary outcome, using the same independent variables and models as shown in Table 6. In this type of graph, better results have greater area-under-the-curve (AUC) scores, implying that they achieve a higher success rate in predictability. Therefore, with a higher AUC score, one can have more faith in the model's reliability.

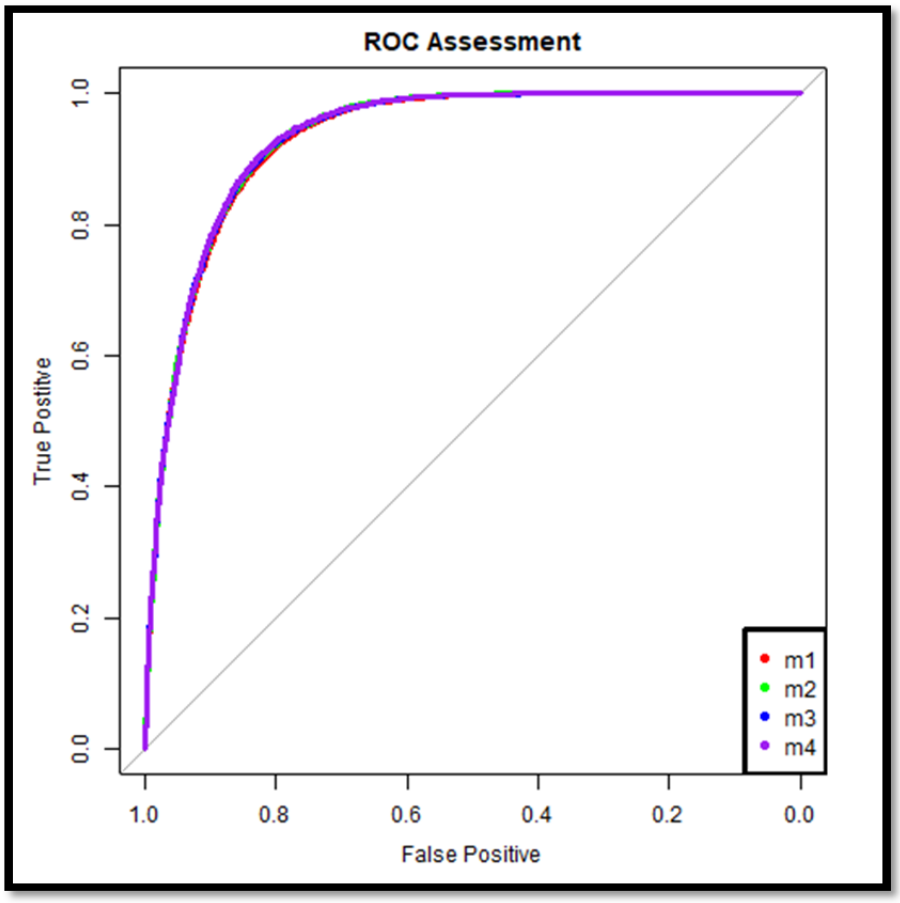


Figure 35. ROC Analysis

The ROC Analysis (Figure 35) shows that the four models yield a similar predictive capability (AUC scores were nearly identical with Model 4 obtaining the best score: m1, m2, m3 = 0.9332, m4 = 0.9336). This assessment enables one to state, that *each of these models* could correctly rank the probability of a successful outcome for a particular swarm, against a known amount of enemies, approximately 93% of the time. For base defense purposes, this means that a commander can work with his intelligence and operations staffs to determine what they believe is the most-dangerous and most-likely threat. Once that is established, the staff can conduct risk assessments concerning the likely effectiveness of a swarm as the sole exterior defense. In low-threat environments, this may relegate the need for as many personnel patrolling beyond the base's perimeter. If the threat-assessment is higher (more enemies are expected to be operating in vicinity of the base), a commander may need to increase force postures and the number of patrols, harden defensive fortifications at the base, request additional drones, or request reserve forces to help augment the base's defensive posture. In addition, further refinements suggested in the next section should push the robustness of the overall defensive algorithms, and, accordingly, the corresponding new model's accuracy.

V. CONCLUSION

A. SIGNIFICANT FINDINGS

1. Overall Usefulness of ABM

This study demonstrated that ABM is an effective and efficient tool for modeling and analyzing how a swarm of drones could best support airfield defense. The ability to quickly change behaviors, parameters, and interaction variables makes for a protean modeling environment rich with possibility for both current and future studies. While substantial and significant updates to this model are possible, there are some baseline conclusions that one can draw from this effort.

2. Are Swarms Effective?

According to the results presented here, drone swarms can be an effective method of support to external base defense given the appropriate resources and underlying logistic architecture. This model intentionally severed the support that the swarm could receive from base personnel by not allowing it to pass key information such as known areas of interest, areas to avoid (increases swarm density by limiting operating area), and locations of suspects to investigate or current attackers. This type of support could greatly increase drone effectiveness. Conversely, the enemies in this model, though high in number, are also not optimized and a vigorous study of counter-UAS and advanced infiltration tactics for enemy actors is likely necessary to improve this model.

3. Which Algorithm Should Defenders Use?

With regard to the algorithms and enemies presented in this study, one can conclude that defensive swarms are best implemented in a grid patrol, with dispersed bomber, formation. This type of swarm provides the best acquisition time, find-to-eliminate time, and also increases survivability for the drones themselves. Additionally, the grid-dispersed swarm is easily tailorable to longer-range threats and has closely-defined coverage patterns once the swarm is in execution (as opposed to the rigidity of

the passive defense). Of note, if a commander is able to choose to use 100% armed UAVs, only the Grid Patrol portion of the algorithm is truly relevant.

4. How Many Drones to Deploy

Unfortunately for mission planners and base defenders, it does not appear that the number of enemies the best indicator for how many drones a base needed to deploy to ensure its protection, and a strict force-ratio calculation is not necessarily applicable to solving the problem. If there is only one sniper threatening a base, a swarm of 50 UAVs may still be unable to locate the lone enemy. Conversely, testing in this study shows that swarms of 220 UAVs are able to counter 100 enemies over 93% of the time. Knowing the number of enemies does not entirely drive the answer for how many drones are needed, but it does provide planners with the ability to project the successfulness of the defensive swarm.

Instead of the number of enemies, it seems, rather, that success is based more on the concept of swarm density. This is evidenced by not only the general success of large formations, but even by those depleted of bombers. Formations with smaller-percentages of bombers still provided adequate protection in most cases once there were a sufficient number of UAVs patrolling the area. Therefore, the model implies that, in order to stop 95% of threats, a potential value for the *minimum swarm density* is 5.62 drones per square mile, with at least 40% armed for defensive situations. I arrive at this number by analyzing outputs of multiple models and noting that swarms with bomber percentages below 40% will sometimes score well-below 95% in cases with many adversaries (80-100 enemies). The swarms in this model operated in a 7.5 by 7.5-mile world, but only patrolled 6.8 by 6.8 miles of it based on the enemy's maximum-threat capability (the mortar). Thus, the swarm patrols a 46.24 square-mile-search area. The results presented indicate that a swarm of 260 drones (with 40% bombers) should be capable of obtaining a 95% protection rate (260 / 46.24 = 5.62) over this sized area. The resultant equation, is therefore *Minimum Swarm Size = Operational Area * 5.62*. However, because the model presented here did not consider variation in the size of the defended area, further research

is needed to determine whether this minimum density would be sufficient under alternative circumstances.

B. CONSIDERATIONS AND RECOMMENDATIONS

There are a multitude of directions future modelers and researchers could take with this study and underlying computer code. While this study focused exclusively on military applications, aerial search algorithms could be entirely applicable to areas of interest such as police operations (from riot control to traffic management), land surveys, agriculture, and search and rescue (on land or sea).

1. Prolonged Time of Operations

Future modelers should develop the model further with multiple engagements over prolonged periods of time, thereby testing the logistic requirements for how many drones need to be at an airfield to conduct a swarming defense. This model shows what sizes may be appropriate, but does not truly test the longevity of operations save for the refueling (changing batteries) and rearming logic. Furthermore, this addition to the model would test the C2's ability to hand-off assignments during continuous operations. Finally, adding in multiple waves of enemies (reinforcements or new attacks) will likely illuminate new requirements for search, C2 assignment, and potentially new optimal geometries.

2. Environment

There are many important upgrades to the environment that modelers could implement in future versions of the model. I recommend expanded consideration of the following environmental factors:

- Further subdivide all grid squares to increase realism on drone scanning times and whether they actually are on top of an enemy at the exact time of discovery.
- Add roads and avenues for high-speed ingress (e.g., vehicle-borne improvised explosive devices).

- Further define the terrain to add more agents (dense woods, hills, caves, swamps, etc.). The enemies would then be affected with decreased visibility, increased or decreased mobility, or even be able to pass through some regions (like caves) completely undetected. The swarm must then be optimized to understand the exact terrain surrounding the base and understand that watching the entries and exits from these important terrain features is critical to area defense.

3. Analysis of Deterrence Factors

While this model analyzed the ability to kinetically defeat the opposition, it completely ignores any deterrent value a swarm may have concerning base defense. It is possible that some actors would be deterred by a persistent swarm guarding a base. However, no defense is impenetrable nor so daunting that dedicated actors would not innovate a way to continue their attack. Thus, the appropriate questions to ask may be what types of attacks will become less likely, and what type of attacks does a swarm enable?

4. Ethical and Safety Concerns for Grenades Overhead

Drones may physically fail, be shot down, or experience artificial-intelligence errors that lead to performing inappropriate actions. In these instances, how safe is it to have hundreds of, potentially armed, actors flying over friendly or non-combatant populations? This model focused on a remote outpost where there was limited concern over a drone failure due to the lack of civilian population near the base. In cases where there are more civilians, is it permissible to chance having armament on commercial-grade hardware overhead civilians? More fundamentally, further research will be required to determine the appropriate engagement criteria for drones.

5. Dynamic Swarm Resizing

Future models should also account for dynamic swarm resizing, especially if modeling multiple waves of enemies or logistics. This can be as simple as increasing the search area for each drone based on how many are airborne (potentially highly

inefficient) or recalculating the appropriate grid dispersion. In recalculating, however, modelers must be aware that due to the continuously changing numbers of drones available for patrol (due to death, a need to RTB, or already assigned to a target), that reassigning drones to separate spots may lead to inefficiencies in swarm behavior. Drones on patrol could end up spending more time moving to their newly assigned locations and less time actively patrolling an area.

6. Remove the C2

It may be entirely beneficial, both to complexity and overall demand on computer hardware, to remove the C2 agent and allow the agents to solve the problems themselves. Although this behavior would be interesting, and potentially desirable, my analysis of the initial algorithms suggested that a central controller would be necessary to ensure that bombers were re-allocated based on threats, especially ones that may be outside of the communications range of a drone on the opposite side of the formation.

For that problem, I considered using a relay amongst the drones but concluded there would be too many signals and instructions for the individual agents to continuously parse. However, as implemented, it is still complicated to monitor and assign everything with a central controller. A better solution may be to simply have the drones attempt to maintain a minimum or maximum distance from one another to create automatic expansions from and collapses towards the base as a swarm (though this could leave the perimeter exposed to incoming mortar or other long-range attacks). It is certainly a possibility to implement and a non-C2 solution may result in phenomena like the emergent properties discussed in chapter two.

C. IMPACT ON SOF AND FUTURE APPLICATIONS

The U.S. Special Operations Command is actively fielding drone technology that can support the warfighter. Versprille reports, “Everything is being considered - from a macro-sized unmanned aerial vehicle weighing 20 pounds or less, up to an MQ-9 sized

capability, which weighs 4,900 pounds without a payload."[79] Regardless of the chosen platform, the requirement for the vehicle to be "flexible, adaptable and proficient"[80] remains. For a UAV to truly support SOF operators, it must have similar characteristics to the force, and mission, it is assisting.

Based on the analysis above, I would argue that small drones, ranging from palm sized to medium quad-copters (approximately 15–30 inches in diameter), can be the next iteration of organic ISR and limited strike. Engineers and designers could augment a drone's inherent capability by adding an ability to link drones together into groups, or swarms. Singular drones, carrying a payload of a high-definition camera and a small weapon (grenade, shape-charge, etc.), or even a swarm working in concert, would provide SOF operators with a solution tailorable at the tactical level to support the team's specific needs given a set mission, operating area, or other mission-related variables.

In tactical situations, these small drones could work as forward ISR elements, base perimeter patrol and defense sentries, or as a new method of fires in kinetic fights. Advances in optics and wireless networking allow for smaller drones to conduct advanced surveillance and engagement profiles. Technologies, such as "Convolutional Neural Networks … allow UAVs to detect hundreds of object categories"[81] and cloud-computing infrastructure enable these drones to perform a vast array of tasks at an incredibly efficient and effective rate.[82] Increases in small motor power and battery performance have also increased flight-dynamic envelopes, loiter time, and operational payload capacity. All of the aforementioned fields still expect significant growth in the next decade so one can assume a correlated rise in drone capabilities.

---

79 Allyson Versprille, "Affordable Surveillance a Priority for Special Operations," *National Defense*, no. 746 (January 1, 2016), http://search.proquest.com/docview/1759029995/.

80 Versprille, "Affordable Surveillance."

81 Jangwon Lee, Jingya Wang, David Crandall, Selma Šabanović, and Geoffrey Fox, "Real-Time, Cloud-Based Object Detection for Unmanned Aerial Vehicles." Extracted from *2017 First IEEE International Conference on Robotic Computing (IRC),* (Taichung, 2017), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7926512&isnumber=7926477, 6.

82 Lee et al., "Real-Time," 1–7.

Combat operations will also benefit from the scalability of drones. A singular drone may be most appropriate to a small team's operations, but in larger-scale conflicts, SOF forces should still benefit from the increased ISR, fires, and support functions that a swarm could deliver. Futurists postulate that "Swarms of low-priced, autonomous drones can operate in a hostile environment, because they can be collectively programmed to undertake all types of emergent behavior (search, swarm to attack, relay information, spook surveillance systems)."[83] Thus, SOF forces may increasingly be able to get "effects" without having to rely on major theater assets. SOF teams using small drones will likely be able to get a particular effect without theater commanders worrying about losing an expensive asset in a heavily contested region or the team fearing being exposed by a larger air platform on a sensitive operation.

For humanitarian or non-combat civil affairs missions, important distinctions may need to be made about the type of drones supporting the mission. During a UN mission in Africa, due to concern over whether the use of ISR drones would incite fear of airstrikes, "UN headquarters [referred to their assets as] Unarmed Unmanned Aerial Vehicles (UUAVs) and deliberately avoided the term drones."[84] Such a simple point of clarification may be essential and effective in humanitarian or peacekeeping support missions. However, it could be necessary to have altogether different equipment. Dorn and Webb believe, "According to the principle of 'humanitarian space', there should be a clear separation of physical aircraft by purpose, as mixing humanitarian and military/intelligence flights would be a 'clear compromise of neutrality', especially in missions where the UN is carrying out combat operations."[85] This same logic could be applied to U.S. forces operating unilaterally or as part of a coalition.

---

83 James J. Wirtz, "The 'Terminator Conundrum' and the Future of Drone Warfare," *Intelligence and National Security* 32, no. 4 (June 7, 2017): 434, http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

84 A. Walter Dorn and Stewart Webb, "Eyes in the Sky for Peacekeeping: the Emergence of UAVs in UN Operations," *Intelligence and National Security* 32, no. 4 (June 7, 2017): 413, http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

85 Dorn and Webb, "Eyes," 415.

Outside of kinetic and ISR capabilities, swarms of drones could also act as a relay for secure beyond-line-of-sight (BLOS) communications. Jeoun writes, "A solution for the communication requirements to enable C2 is the utilization of mobile wireless networks with UAV relays to increase the effectiveness of a SOF unit."[86] Figure 36 shows how a swarm of drones could support disparate elements utilizing a communication's architecture supported by UAVs. A network like this could be preferable to using satellite communication in cases of limited bandwidth or an enemy jamming the low-power satellite link.

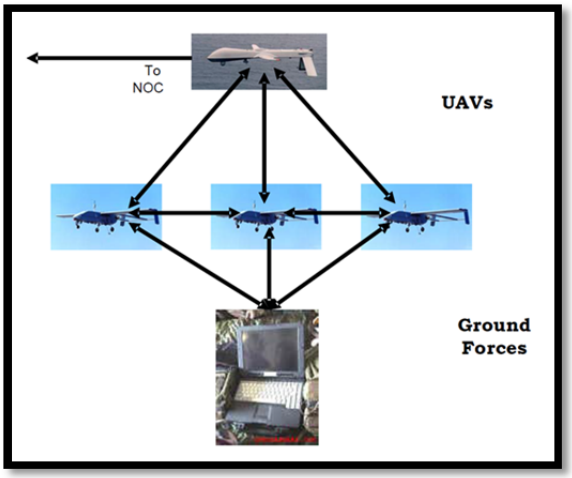


Figure 36. Network Operations Center (NOC) Communications Relay[87]

Regardless of which mission drones are used for or how they are employed, it is important to recognize that drone technology is rapidly improving and will be present in (virtually) all foreseeable future operations. Additionally, artificial intelligence (AI), via computer learning and image recognition, will soon support these missions at exponentially greater magnitudes due to advances in computing power and networking. Wirtz discuses, "Field experimentation also has revealed that the performance of fully

86 Kristina S. Jeoun, "The Tactical Network Operations Communication Coordinator in Mobile UAV Networks," (Naval Postgraduate School, 2004), 3.

87 Exact image borrowed from: Jeoun, "Tactical Network," 7.

autonomous drones will probably exceed the performance of their human-piloted counterparts in counter-terror missions."[88] With increased capability, the only remaining debate will be over ethical concerns of computer-directed hostile engagement, which may also soon subside as AI and robots become more integrated into mainstream society.

Opponents will suggest that "Drones lack the endurance or the search aperture to acquire targets through random surveillance of some countryside and, instead, rely on a massive intelligence infrastructure to be vectored toward likely targets."[89] However, drones working in support of SOF do not need to cover as much terrain and will likely be used in more discreet or limited missions where there is a known target or smaller area of operations. Others will suggest that because an advanced drone like the MQ-9 is so costly,[90] it is simply too expensive to procure enough assets to support each individual unit. This critique is valid but also emphasizes why the answer could be to procure small, cheap, disposable drones. A SOF team cannot employ an MQ-9 without a massive logistic footprint or additional personnel to physically operate and maintain the vehicle. This is too large of a requirement and often provides excessive capability or worse yet, may not be capable of supporting a small, covert action.

Finally, the ability to conduct kinetic strikes from drones of any size does not create a ubiquitous solution. The success of SOF actions, "along with policymakers' reliance on raids and drones, has encouraged a misperception of such actions as quick, easy solutions that allow Washington to avoid prolonged, messy wars."[91] The truth is far from it. One does not need to have mastered Arreguín-Toft's theories[92] to know that small kinetic attacks will not win over a populace, nor defeat insurgents or conventional forces. In the case of SOF, drones should be used in support of limited DA missions or as part of a defensive network while SOF forces establish "long-term relationships fostered

---

88 Wirtz, "Terminator Conundrum," 434.

89 Wirtz, "Terminator Conundrum," 434.

90 $64.2 million (FY 2006) according to Versprille, "Affordable Surveillance."

91 Linda Robinson, "The Future of Special Operations," *Foreign Affairs* 91, no. 6 (2012): 111.

92 Ivan Arreguín-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (Summer 2001): 93–128.

by the indirect approach [which generate] conduits for understanding and influence."[93] The people are still an inextricable part of the mission.

Ultimately, UAVs are certainly an important part of the future of air combat and support. "Technological developments will make drones fly faster, higher, for longer periods of time, and capable of carrying a variety of different payloads …. Drones are much cheaper than ordinary aircraft, both in purchase price and in maintenance."[94] Since the U.S. military leadership has already identified that UAVs can create a decisive advantage, it is incumbent on acquisitions personnel to work with operators to ensure that the right equipment is sought after, and not just the most capable. Being able to place hundreds of "capability-limited" drones out in defense of an airbase, to send a few out with each deployed SOF team, or simply allowing users to operate them without fear of reprisal should the units become damaged has potentially greater upside than getting a few top-tier UAV platforms. As the saying goes, "Quantity has a quality all its own."[95]

---

93 Robinson, "The Future of Special Operations," 114.

94 Shlomo Shpiro, "Seeing but unseen: intelligence drones in Israel," *Intelligence and National Security* 32, no. 4 (June 7, 2017), 429, http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

95 Often attributed to Joseph Stalin but may be more accurately linked to Thomas Callaghan Jr., a defense consultant in the U.S. during the 1970s and 1980s.

APPENDIX. PYTHON CODE EXPLANATIONS

A. MODEL

The Model file is where the specific base, environment, agents, and data collection are created. This file receives the inputs from the Server file and any updated User-Settable Parameters. Once created the Model creates a randomized order each step (time unit), and allows each agent to effectively have a turn to choose what it will do. The randomly-selected agents then accomplish their turn logic sequentially, and once all agents have chosen an action, the GUI is updated and the model moves to the next step.

B. AGENT

The Agent file is where the individual ABM logic is defined. Each type of agent in the simulation is coded into a distinct class. A class is a staple data-type of object-oriented programming (OOP). I use class structures to define the attributes, states, and capabilities for any given type of agent (drones, mountains, command and control, snipers, etc.). This type of programming provides the designer with the ability to create multiple instances (each an "object") of a Class which all have the same inherent attributes, but yet are distinct.

Mesa provides basic Agent capabilities (create, add to schedule, know what is in the surrounding squares, its "neighborhood"). I created the "Operator" class to serve as the main parent class for many of the other classes; in OOP, the classes that use logic from a parent class are referred to as extensions or child classes. Here, Agent is Operator's parent, and the specific actors in the model are all extensions of Operator. It provides common functionality for both protagonists (Base, Command and Control, Drone) and antagonists (Enemy, Sniper, Mortar, UAV).

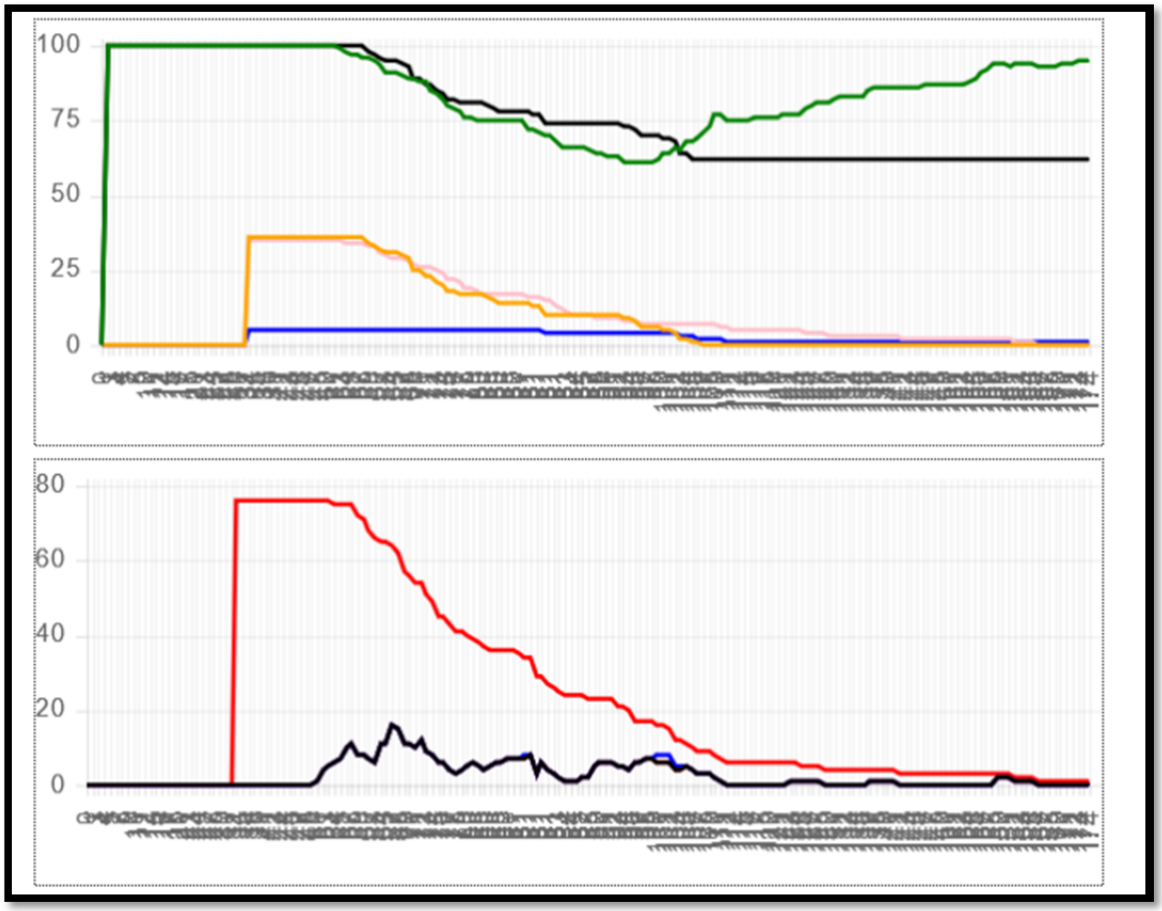
In the model, all drones, defined as *seekers* (no grenades) and *bombers* (those with grenades) are inherently the same, but individually have different states of available fuel or grenades based on what has happened to that particular instance of a drone. This is an essential piece of my design. Because of the structured class system in my code, it is incredibly simple to scale the number of actors in the model. Each specific instance of an

agent is created with a unique identification number (ID) so that my software can track which agents are currently performing certain actions. Mesa uses that same ID to ensure that each agent gets a turn on every step.

C. SERVER

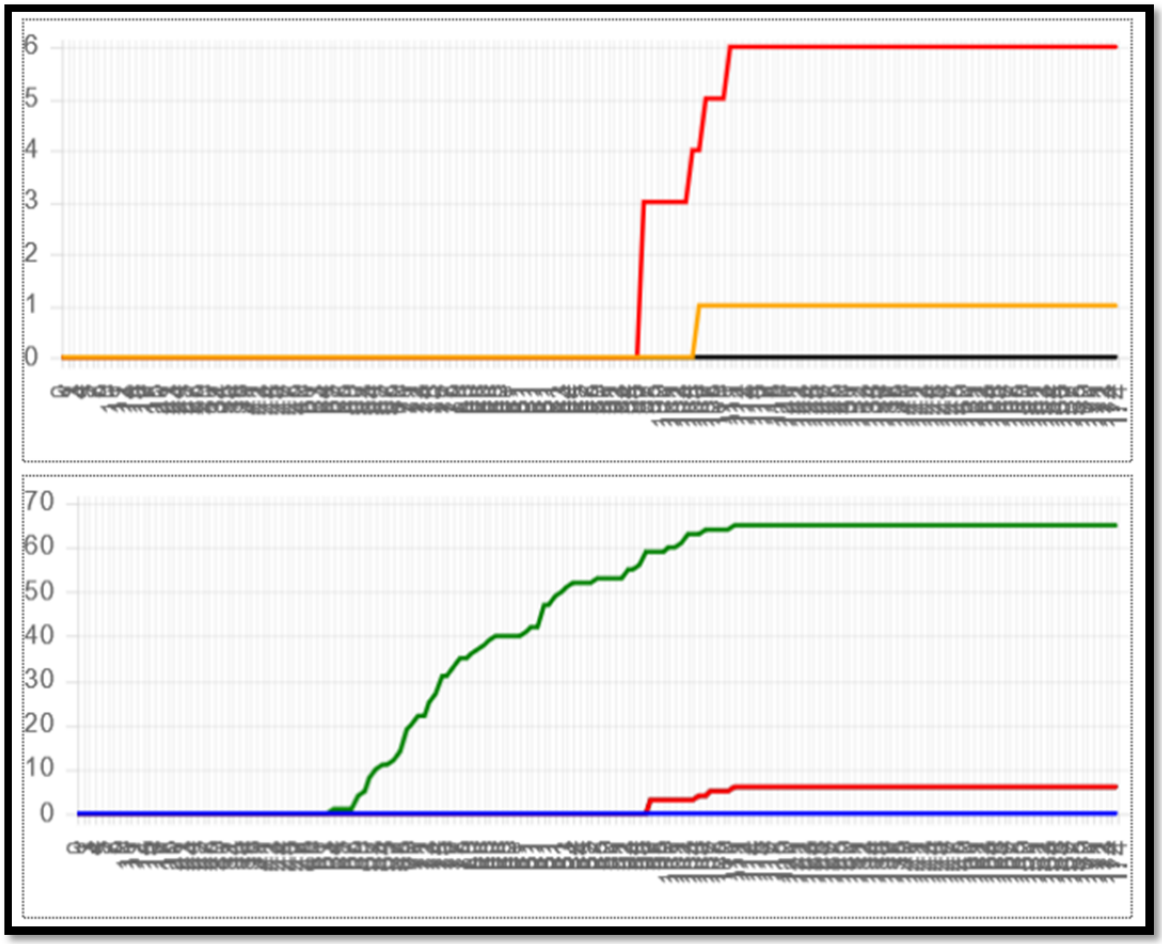
I use the Server file to create the actual representation of the model. This is the graphical-user interface (GUI) that the user actually sees on her monitor.[96] This file controls the specific depiction of all the different actors as well as defining what variables the model will collect and graph during execution. Finally, the Server file is where the initial conditions for all "User-Settable Parameters," as Mesa calls them, are set. In a single-run instance, all of these variables can be changed once the model's webpage is created (by running the model). The types of parameters include drop-down menus, switches, and sliders that allow the user to define the number of a particular object at the model's outset.

[96] Unless they use the "batch-run" process, which then provides no GUI.



These first two graphs appear below the gridded area depicting the interactions. The server file defines which variables to show in these real-time charts. The top graph shows the size of the drone force (black and green for seekers and bombers), and the enemy forces. The bottom graph depicts the presence of enemies along with the C2's current awareness of threats that the drones are tracking or targeting.

Figure 37. Swarm and Enemy Forces



The final two graphs depict the current results of the simulation at the present step. The top graph shows the number of successful mortar and sniper attacks (red, black), as well as how many enemy UAVs were able to penetrate the base's perimeter (orange). The bottom graph shows the number of enemies stopped by the swarm (green) and the number of unique mortar and sniper attacks (red and blue).

Figure 38. Real-Time Results Tracking

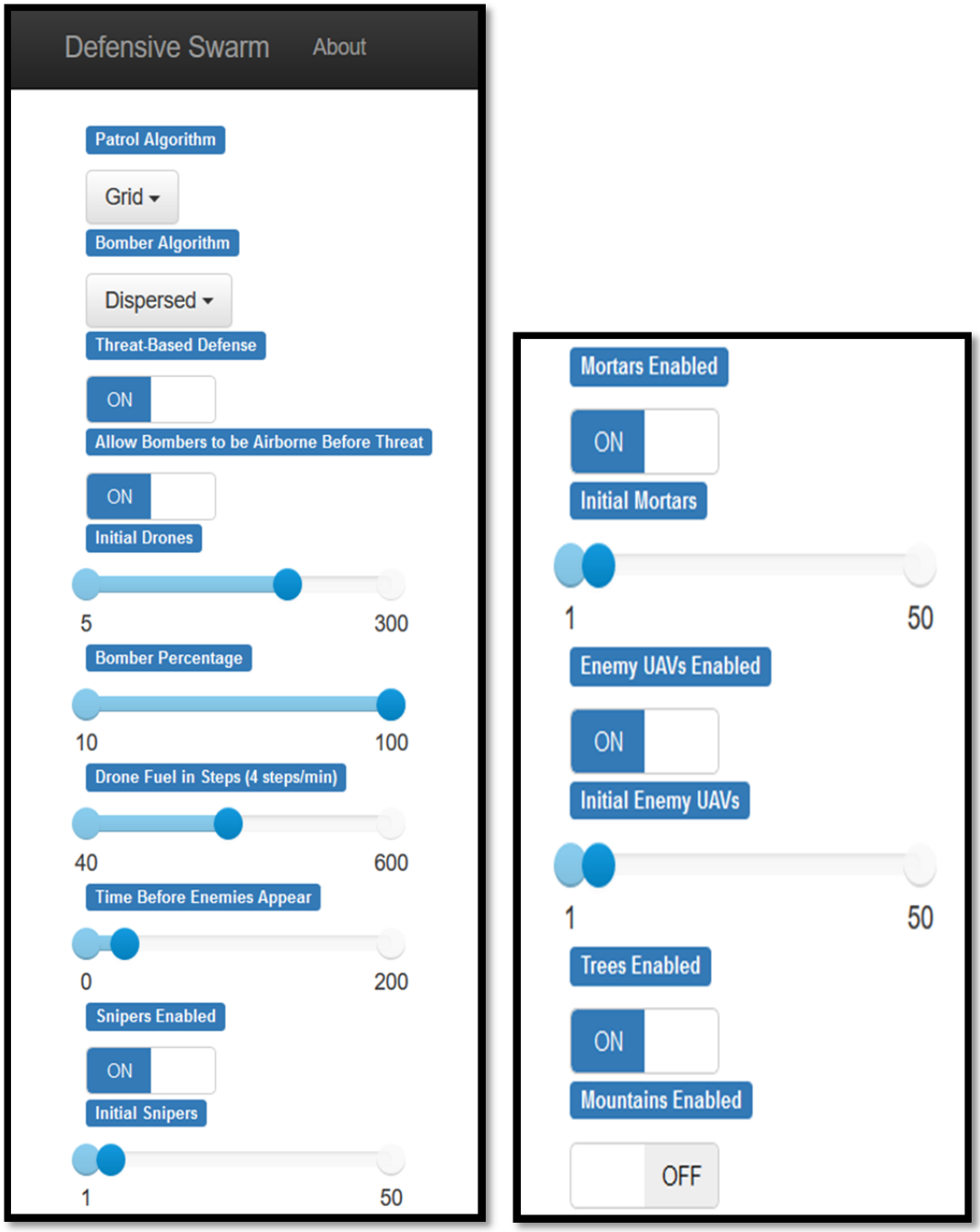


Figure 39. User-Settable Parameters in Defensive-Swarm Model

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Theodore T. *Introduction to Discrete Event Simulation and Agent-based Modeling: Voting Systems, Health Care, Military, and Manufacturing*. London; New York: Springer, 2011. https://link.springer.com.libproxy.nps.edu/book/10.1007/978-0-85729-139-4.

Arreguín-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26, no. 1 (Summer 2001): 93–128. http://www.jstor.org.libproxy.nps.edu/stable/3092079.

Arquilla, John. "The Coming Swarm." *New York Times*. February 14, 2009. http://www.nytimes.com/2009/02/15/opinion/15arquilla.html.

Arquilla, John, and David Ronfeldt. *Swarming and the Future of Conflict*. Santa Monica, CA: RAND Corporation, 2000. http://www.rand.org/pubs/documented_briefings/DB311.html.

Austin, Reg. *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. New York: John Wiley & Sons, Incorporated, 2010. ProQuest Ebook Central. https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=514439.

Buonaugurio, Michael P. "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision." Master's thesis, Marine Corps Command and Staff College, 2001. http://handle.dtic.mil/100.2/ADA401262.

Byman, Daniel L. "Why Drones Work: The Case for Washington's Weapon of Choice." June 17, 2013. Brookings. https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice.

Christensen, Glen E. "Air Base Defense in the Twenty-First Century." Master's thesis, U.S. Army Command and General Staff College, School of Advanced Military Studies, 2007. http://www.dtic.mil/docs/citations/ADA470671.

Christie, Mike, Andrew Cliffe, Philip Dawid, and Stephen S. Senn, eds. *Simplicity, Complexity and Modelling*. New York: John Wiley & Sons, Incorporated, 2011. ProQuest Ebook Central. https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=819164.

Covault, Shawn C. "Enhancing Air Base Defense Through Joint Doctrine." Master's thesis, Marine Corps Command and Staff College, 2009. http://handle.dtic.mil/100.2/ADA510273.

Department of Defense. “Department of Defense Announces Successful Micro-Drone Demonstration Press Operations.” Release No: NR-008-17, January 9, 2017. https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration.

Department of the Army. *FM 3–21.38 Pathfinder Operations.* April 2006. http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm3_21x38.pdf.

Ditlevson, Jeffery T. ”Air Base Defense: Different Times Call for Different Methods.” Master’s thesis, Naval Postgraduate School, 2006. https://calhoun.nps.edu/bitstream/handle/10945/2508/06Dec_Ditlevson.pdf?sequence=1.

DJI. “Phantom 4.” 2017. https://www.dji.com/phantom-4.

Dorn, A. Walter, and Stewart Webb. “Eyes in the Sky for Peacekeeping: the Emergence of UAVs in UN Operations.” *Intelligence and National Security* 32, no. 4 (June 7, 2017). http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

Drone Labs LLC. “How We Compare.” 2017. http://dronedetector.com/compare-detection-systems.

Efron, Shira. *The Use of Unmanned Aerial Systems for Agriculture in Africa: Can It Fly?* Santa Monica, CA: RAND Corporation, 2015. http://www.rand.org/pubs/rgs_dissertations/RGSD359.html.

Gazi, Veysel, and Baris Fidan. “Coordination and Control of Multi-agent Dynamic Systems: Models and Approaches.” In *Swarm Robotics: SAB 2006 International Workshop: Revised Selected Papers*, edited by Erol Şahin, William M. Spears, and Alan F. T. Winfield, 71–102. Berlin; New York: Springer, 2007. https://link.springer.com.libproxy.nps.edu/chapter/10.1007/978-3-540-71541-2_6.

Gibbons-Neff, Thomas. “ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say.” *The Washington Post*, June 14, 2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-dronesare-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/?utm_term=.3e1b890ed203.

Gonzales, Dan, and Sarah Harting. *Designing Unmanned Systems with Greater Autonomy: Using a Federated, Partially Open Systems Architecture Approach*. Santa Monica, CA: RAND Corporation, 2014. http://www.rand.org/pubs/research_reports/RR626.html.

Gray, Ron. ”Integrated Swarming Operations for Air Base Defense Applications in Irregular Warfare.” Master’s thesis, Naval Postgraduate School, 2006. http://library.nps.navy.mil/uhtbin/hyperion/06Jun_Gray.pdf.

Howard, Stephen P. "Special Operations Forces and unmanned aerial vehicles : sooner or later?" Maxwell Air Force Base, Alabama: Air University Press, School of Advanced Airpower Studies, 1996. http://aupress.maxwell.af.mil/digital/pdf/paper/t_howard_special_operations_forces.pdf.

Hubbard, Curtis W. "Base Defense at the Special Forces Forward Operating Base." Thesis, U.S. Army Command and General Staff College, 2002. http://handle.dtic.mil/100.2/ADA407001.

Jane's Defence Equipment & Technology Intelligence Centre. "2B14 Podnos 82 mm light mortar." Jane's by IHS Markit. 2017. https://janes.ihs.com.libproxy.nps.edu/Janes/Display/jiw_0909-jiw.

Jeoun, Kristina S. "The Tactical Network Operations Communication Coordinator in Mobile UAV Networks." Master's thesis, Naval Postgraduate School, 2004. http://hdl.handle.net/10945/1570.

Joint Chiefs of Staff. "The National Military Strategy of the United States of America 2015." Washington, D.C.: Joint Staff Publications, June 2015. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

Joint Staff. *Joint Publication 3–05 Special Operations*. Joint Electronic Library, July 16, 2014. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.

Joint Staff. *Joint Publication 3–10 Joint Security Operations in Theater*. Joint Electronic Library, November 13, 2014. http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.

Lee, Jangwon, Jingya Wang, David Crandall, Selma Šabanović, and Geoffrey Fox. "Real-Time, Cloud-Based Object Detection for Unmanned Aerial Vehicles." Extracted from *2017 First IEEE International Conference on Robotic Computing (IRC)*. Taichung, 2017. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7926512&isnumber=7926477.

Macal, Charles, and Michael North. "Agent-Based Modeling and Simulation: ABMS examples." In *Proceedings of the 2008 Winter Simulation Conference*, 2008.

Mesa Team. "Mesa: Agent-Based Modeling in Python 3+." 2017. http://mesa.readthedocs.io/en/master/.

Ministry of Defence and Philip Dunne. "Miniature Surveillance Helicopters Help Protect Front Line Troops." *Government of the United Kingdom*. February 4, 2013. https://www.gov.uk/government/news/miniature-surveillance-helicopters-help-protect-front-line-troops.

National Geospatial-Intelligence Agency. "Universal Grids and Grid Reference Systems, Version 2.0.0." February 28, 2014. http://earth-info.nga.mil/GandG/update/coordsys/resources/NGA.STND.0037_2.0.0_GRIDS.pdf.

Obama, Barack. "National Security Strategy 2015." Washington, D.C.: Executive Office of the President February, 2015. http://nssarchive.us/national-security-strategy-2015/.

Penny, Maryse, Tess Hellgren, and Matt Bassford. *Future Technology Landscapes: Insights, Analysis and Implications for Defence*. Santa Monica, CA: RAND Corporation, 2013. http://www.rand.org/pubs/research_reports/RR478.html.

Peters, John E., Somi Seong, Aimee Bower, Harun Dogo, Aaron L. Martin, and Christopher G. Pernin. *Unmanned Aircraft Systems for Logistics Applications.* Santa Monica, CA: RAND Corporation, 2011. https://www.rand.org/pubs/monographs/MG978.html.

Python Software Foundation. "Python." 2017. https://www.python.org/.

The R Foundation. "The R Project for Statistical Computing." 2017. https://www.r-project.org/about.html.

Robinson, Linda. "The Future of Special Operations." *Foreign Affairs* 91, no. 6 (2012): 110–122. http://web.b.ebscohost.com.libproxy.nps.edu/ehost/detail/detail?vid=1&sid=ccf70875-b292-4669-a006-dd038f94078b%40pdc-v-sessmgr01&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=82763903&db=bth.

Schmickl, Thomas, Christoph Möslinger, and Karl Crailsheim. "Collective Perception in a Robot Swarm." In *Swarm Robotics: SAB 2006 International Workshop: Revised Selected Papers*, edited by Erol Şahin, William M. Spears, and Alan F.T. Winfield, 144–157. Berlin; New York: Springer, 2007. https://link.springer.com.libproxy.nps.edu/chapter/10.1007/978-3-540-71541-2_10.

Schneider, Michael Matthew. "An Investigation of Alternative Deployment Doctrines for an Integrated Sensor Array in Base Defense." Master's thesis, Naval Postgraduate School, 1971. http://hdl.handle.net/10945/15770.

Shlapak, David A., and Alan J. Vick. "*Check Six Begins on the Ground:" Responding to the Evolving Ground Threat to U.S. Air Force Bases*. Santa Monica, CA: RAND Corporation, 1995. http://www.rand.org/pubs/monograph_reports/MR606.html.

Shpiro, Shlomo. “Seeing but unseen: intelligence drones in Israel.” *Intelligence and National Security* 32, no. 4 (June 7, 2017). http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

Tan, Hock Woo. ”Agent-based Model and System Dynamics Model for Peace-keeping Operations.” Master’s thesis, Naval Postgraduate School, 2014. http://hdl.handle.net/10945/44010.

United States Army Acquisitions Support Center. “Counter-Rocket, Artillery, Mortar (C-RAM) Intercept Land-Based Phalanx Weapon System (LPWS).” http://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/.

Versprille, Allyson. “Affordable Surveillance a Priority for Special Operations.” *National Defense*, no. 746 (January 1, 2016). http://search.proquest.com/docview/1759029995/.

Vicomtech-IK4. “Real Time Detection of Events for Surveillance Applications.” 2013. http://www.viulib.org/solutions/s24/real_time_detection_of_events_for_surveillance_applications.

Vick, Alan. *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges*. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR968.html.

Wirtz, James J. “The ‘Terminator Conundrum’ and the Future of Drone Warfare.” *Intelligence and National Security* 32, no. 4 (June 7, 2017). http://dx.doi.org.libproxy.nps.edu/10.1080/02684527.2017.1303127.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California